

УДК 004.9

О ПРИКЛАДНЫХ АСПЕКТАХ ПРИМЕНЕНИЯ М-МАТРИЦ

Ю. Н. Балонин,
инженер

А. А. Востриков,
канд. техн. наук

М. Б. Сергеев,

доктор техн. наук, профессор

Санкт-Петербургский государственный университет аэрокосмического приборостроения

Рассматриваются свойства ортогональных минимаксных М-матриц, затрагивающие аспекты их прикладного использования для кодирования и маскирования изображений.

Ключевые слова — ортогональные минимаксные матрицы, М-матрицы, матрицы Адамара, матрицы Белевича, маскирование изображений.

В работе [1] предложен способ маскирования цифровых изображений, обеспечивающий их конфиденциальность при передаче по каналам сетей общего пользования. Способ основан на применении аппарата матричного преобразования тела изображения, производимого с использованием уникальной матрицы, поиск которой представляет значительную вычислительную сложность [2].

В работах [3–5] описан класс минимаксных М-матриц, являющихся ортогональными матрицами с минимальным максимальным по абсолютной величине элементом. Важными представителями этого класса являются матрицы Адамара [6–8] и Белевича [9].

Указанные ортогональные матрицы связаны с нахождением спектров сигналов и заменяют матрицу преобразования Фурье в частных случаях обработки дискретных сигналов. По отношению к матрицам Адамара, имеющим всего два уровня значений элементов $\{1, -1\}$, М-матрицы допускают большее число уровней — $\{a, b, c, d, \dots\}$. Несмотря на то, что эти новые матрицы оптимальны в строгом математическом смысле, как и матрицы Адамара, это все же некоторое послабление в сторону более мягкой дискретизации уровней гармонических базисных функций, представленных после специфического квантования столбцами М-матрицы.

Применение матриц Адамара закрепилось в практике помехоустойчивого кодирования. Например, в космической индустрии с ними связана история передач первых снимков Юпитера, Сатурна удаленными космическими аппаратами

[10]. Кратко пояснить целесообразность передачи спектров, а не самих сигналов, можно тем, что одиночная радиопомеха (всплеск) на спектре приведет после обратного преобразования, согласно равенству Парсевала, всего лишь к легкой ряби снимка. Причем импульс помехи в начале передачи кадра даст низкочастотный шум, тогда как в конце — синусное искажение высокой частоты и малой амплитуды. Перестановкой столбцов нормализованной матрицы можно менять характер проявления искажения.

До тех пор, пока обрабатывающие изображение процессоры были маломощны, для реализуемости подхода определенное значение играла двухуровневость матрицы Адамара, обеспечивающая небольшую вычислительную сложность процедуры обработки изображений. Сегодня, с увеличением их производительности, этот фактор отходит на второй план, и в технологии кодирования и маскирования может быть использован весь набор матриц, включая n -уровневые М-матрицы.

Связь М-матриц с теорией защиты информации была обнаружена благодаря работам В. Белевича. В работе [3] опубликована М-матрица 22-го порядка, замещающая отсутствующую С-матрицу Белевича, нахождение которой связано со значительными вычислительными затратами ввиду сверхчувствительности алгоритма к начальным условиям.

Перечислим, помимо математических аспектов, аргументы в пользу целесообразности применения М-матриц для помехоустойчивого кодирования и защиты информации.

Прежде всего, эти матрицы, по сравнению с матрицами Адамара, новы и изучены значительно меньше. Это означает дополнительные трудности поиска M , поскольку подход неизвестен или малоизвестен. Как и все ортогональные матрицы, они имеют преимущество хорошей обусловленности для проведения математических операций обработки сигналов. Их n -уровневость наследует крайне усеченное проявление этого свойства у матриц Адамара. Вместо двух целых уровней $\{1, -1\}$ имеем целые или, при повышении порядка, иррациональные значения n уровней. Для хранения таких матриц в памяти процессоров достаточно штампов поэлементно заданной структуры. Иррациональность уровней — лишь дополнительный аргумент к приведенным выше. Вычислять значения уровней можно по найденным аналитическим формулам [3, 4].

Конечно, M -матрицы — некоторый компромисс между помехоустойчивостью, максимальной у матриц Адамара, и информационной защищенностью, поскольку они имеют больше факторов влияния на процесс построения эвристических алгоритмов, дополнительной вариативно-

сти. Перечислять эвристические приемы не имеет смысла ввиду их очевидного разнообразия. Всего лишь тривиальная перестановка строк и столбцов не меняет ортогональности матрицы (инвариантная операция) и порождает большое количество вариантов, зависящее от порядка матрицы. Порядок же может быть выбран сколь угодно большим. Тем самым M -матрицы, безусловно, интересный объект и для теории, и для практики помехоустойчивого и помехозащитного кодирования.

Результаты проводимых исследований позволили дополнить постоянно ведущийся мониторинг M -матриц [11] континуальными семействами уровней матриц, представителями которых являются, в том числе, регулярные (правильные уровневые) решения и оптимальные M -матрицы.

В заключение отметим, что работа по поиску, исследованию основных свойств M -матриц важна для становления новой ветви прикладного использования матриц Адамара в их обобщении на нечетные и некоторые исключительные четные порядки.

Литература

1. **Ерош И. Л., Сергеев М. Б., Филатов Г. П.** О защите цифровых изображений при передаче по каналам связи // Информационно-управляющие системы. 2007. № 5. С. 20–22.
2. **Eroch I., Sergeev M.** Fast encryption of various types of messages // Mechanical Engineering. 2007. Vol. 51. N 1. P. 1–10.
3. **Балонин Ю. Н., Сергеев М. Б.** M -матрица 22-го порядка // Информационно-управляющие системы. 2011. № 5. С. 87–90.
4. **Балонин Н. А., Сергеев М. Б.** M -матрицы // Информационно-управляющие системы. 2011. № 1. С. 14–21.
5. **Балонин Н. А., Мироновский Л. А.** Матрицы Адамара нечетного порядка // Информационно-управляющие системы. 2006. № 3. С. 46–50.
6. **Hadamard J.** Resolution d'une question relative aux determinants // Bull. sci. math. 1893. Vol. 2. P. 240–248.
7. **Paley R. E. A. C.** On orthogonal matrices // J. Math. Phys. 1933. N 12. P. 311–320.
8. **Мониторинг** матриц Адамара. <http://mathworld.wolfram.com/HadamardMatrix.html> (дата обращения: 10.02.2012).
9. **Belevitch V.** Theory of $2n$ -terminal networks with applications to conference telephony // Electrical Communication. 1950. Vol. 27. P. 231–244.
10. **Van Lint J. H., Seidel J. J.** Equilateral point sets in elliptic geometry // Indagationes Mathematicae. 1966. Vol. 28. P. 335–348.
11. **Мониторинг** M -матриц. <http://mathscinet.ru> (дата обращения: 10.02.2012).

ПРОЕКТ СОЗДАНИЯ МЕЖДУНАРОДНОЙ АЭРОКОСМИЧЕСКОЙ СИСТЕМЫ ГЛОБАЛЬНОГО МОНИТОРИНГА: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РЕАЛИЗАЦИИ

Международная аэрокосмическая система глобального мониторинга (МАКСМ) — это инициатива российских научных и общественных организаций по созданию «системы систем», предназначенной для эффективного предупреждения мирового сообщества о грозящих угрозах глобального характера, в том числе космического происхождения. Землетрясение в Новой Зеландии и сейсмосообщения в Японии подтвердили актуальность МАКСМ. Достигнутые результаты в реализации проекта можно разделить на три большие группы: научно-технические, политические и организационные.

Выполненные обширные научно-технические исследования по обоснованию будущей системы полностью подтвердили техническую реализуемость основных идей, заложенных в ее основу.

МАКСМ должна создаваться и развиваться на принципах поэтапного формирования глобальной сети, интегрирующей в своем составе наряду с уже существующими информационно-навигационными и телекоммуникационными ресурсами традиционных космических систем нацио-

нальной, региональной и международной принадлежности специализированный прогнозный, мониторинговый потенциал, который должен появиться в ходе реализации основной идеи проекта — эффективного сбора данных о предвестниках стихийных бедствий и техногенных катастроф. В то же время, предоставляя ресурсы в МАКСМ, ее участники получают прямой и безвозмездный доступ ко всей информации, циркулирующей внутри системы.

В рамках разрабатываемого системного проекта МАКСМ предстоит наполнить реальным содержанием ключевые направления работ:

- по обоснованию путей, методов и средств корректной интеграции (технического сопряжения) имеющихся информационных, телекоммуникационных и мониторинговых ресурсов в единую систему;
- по синтезу рационального состава и орбитального построения специализированного космического сегмента МАКСМ с перспективной аппаратурой регистрации предвестников стихийных бедствий и техногенных катастроф;



■ Последствия землетрясений Японии

• по решению вопросов развития наземной инфраструктуры приема, обработки, интеграции, интерпретации и распространения данных прогнозного мониторинга, корректно преобразуемого в информацию предупреждения на международном и национальном уровнях.

Результатом **первого технического направления** работ по проекту должны стать алгоритмы и технологии интеграции в МАКСМ средств и ресурсов, включая их информационное сопряжение, что является хотя и весьма сложной, но решаемой задачей.

Второе направление — создание специализированного космического сегмента МАКСМ — является наиболее сложным. Российские ученые и инженеры достигли реальных успехов в решении задач прогнозирования природных стихийных бедствий. Подтверждением этому служат получивший недавно грант Евросоюза проект ОАО «Российские космические системы» по комплексному мониторингу ионосферы в районе о. Сахалин; разработки специалистов «Научного центра оперативного мониторинга Земли» по анализу конфигурации облачности в преддверии недавних землетрясений в Японии и Новой Зеландии, позволившие спрогнозировать их наступление за несколько часов до начала. Однако, несмотря на достигнутые результаты, пока нельзя говорить о приемлемо достоверном прогнозе магнитуды и времени наступления землетрясений с выходом на задачи предупреждения.

Эффективный прогнозный мониторинг станет возможен лишь при условии дооснащения существующих космических систем новыми геофизическими приборами и средствами оптико-электронного наблюдения во всем диапазоне электромагнитного спектра, которые активно разрабатываются во многих странах мира. Образцы бортовой геофизической аппаратуры, пригодные для монтажа на борту малых и микроспутников, уже созданы в России и апробированы в космосе (КА «Компас-1» и «Компас-2»). На этапе опытно-конструкторских работ находится уникальный отечественный проект мониторинга ионосферы «Геофизика».

Для прогнозирования критических ситуаций техногенной природы потребуется аналогичный состав бортовой аппаратуры, дополненный инструментарием прецизионной геодезической, интерферометрической и стереосъемки из космоса, а также средствами сбора датчиковой информации о состоянии потенциально опасных технических объектов с использованием возможностей группировок систем космической навигации (в частности, ГЛОНАСС).

Руководство проектом рассчитывает на использование научно-технического задела в обла-

сти создания малых КА «САТ-О» в рамках российско-белорусской программы и широкую международную кооперацию. Первые позитивные результаты рабочих контактов с группой профильных канадско-американских (CANEUS), британских (SURREY) и китайских (DFH Satellite Co.Ltd.) компаний дают основания надеяться на продуктивность такого подхода.

Третье магистральное техническое направление работ по проекту — развитие наземной инфраструктуры МАКСМ для приема, обработки, интегрирования, интерпретации и распространения данных прогнозного мониторинга — предполагает решение широчайшего спектра организационно-технических, политических и правовых вопросов.

Иерархическая наземная инфраструктура МАКСМ состоит из трех уровней. Нижний уровень представлен существующими средствами для приема и обработки мониторинговой информации и датчиковыми сетями национальной и региональной принадлежности, которые в перспективе могут быть дополнены и специализированными международными станциями; средний уровень — средствами интерпретации мониторинговых данных национальной и региональной принадлежности; а верхний — международными центрами управления в кризисных ситуациях. Руководство проектом уже провело неформальные консультации с представителями ряда стран (Украины, Камеруна, Китая, Вьетнама, Индонезии) о возможности размещения на их территориях информационной инфраструктуры МАКСМ и получило принципиальную поддержку этой идеи.

Проект уже трижды представлялся на уровне ООН. В результате к нему привлечено внимание ряда стран (Индонезии, Тайваня, Японии) и международных организаций (секретариата ГЕО и Управления ООН по космосу, руководства СПАЙДЕР-ООН).

Особую роль в политическом продвижении идеи МАКСМ играет прошлогодний Вашингтонский саммит руководителей космических агентств, где проекту практически целиком был посвящен один из пленарных докладов.

Цель МАКСМ целиком и полностью поддерживается профильными учреждениями ГЕОСС, а секретариат ГЕО готов начать процедуру официального признания проекта.

Организационный аспект продвижения проекта МАКСМ связан с его поддержкой со стороны Российской академии космонавтики им. К. Э. Циолковского и Международной академии астронавтики. В 2010 г. создан Международный комитет по реализации проекта МАКСМ. Комитет — неправительственная организация, в составе которой 77 официальных членов и наблюдателей,

представляющих более 30 стран и международных организаций.

На заседании Комитета в сентябре 2010 г. в дни работы 61-го Международного конгресса астронавтики были приняты Устав организации, план работы, а также решение о регистрации. Комитет уже заключил более 60 соглашений о сотрудничестве с профильными национальными, региональными и международными организациями.

Комитет подписал соглашения с космическими агентствами Аргентины, Индонезии и Испании, провел переговоры о присоединении к проекту с Китайской национальной космической администрацией, Национальной академией наук Армении, секретариатом АСЕАН и Управлением космической политики в структуре правительства Австралии.

В течение 2010–2011 гг. проект МАКСМ представлялся на научных форумах и переговорах в Риме (Италия), Хайфе (Израиль), Париже (Франция), Бонне (Германия), Риге (Латвия), Стокгольме (Швеция), Донецке (Украина), Пекине (Китай), Москве, Казани (Россия), Праге (Чехия), Вашингтоне (США), Бойе (Камерун), Джакарте (Индонезия), Мельбурне (Австралия), Мадриде (Испания). Особо следует отметить Первую региональную конференцию в Юго-Западной Африке (Камерун), организованную по инициативе Международной академии астронавтики.

Международный специализированный симпозиум «Космос и глобальная безопасность человечества» по тематике МАКСМ проводится в течение года по «диверсифицированной схеме» — в виде отдельных тематических семинаров и круглых столов в рамках научных форумов. На «Международном форуме по проблемам информатизации общества — проблемы, перспективы, инно-

вационные подходы» работает отдельная секция «Проблемы формирования единого информационного ресурса МАКСМ».

Таким образом, достаточно эффективно решаются задачи продвижения проекта за рубежом с необходимым охватом научной аудитории, политических и бизнес-кругов различных стран.

Наряду с позитивными политическими последствиями создания и использования МАКСМ существуют проблемы, связанные с научным и промышленным шпионажем, использованием мониторинговых технологий и информационно-телекоммуникационных ресурсов системы в военно-прикладных целях. Принятие политической декларации с рабочим названием «О консолидации усилий мирового сообщества по использованию аэрокосмического потенциала в интересах предупреждения о природных и техногенных угрозах глобального характера» могло бы послужить делу политической транспарентности МАКСМ.

Создание МАКСМ даст возможность решать широкий спектр общечеловеческих задач, объединить усилия многих стран в рамках новой единой стратегии сугубо мирного освоения космоса, направленной на обеспечение безопасного и социально устойчивого развития мирового сообщества в XXI столетии.

*Меньшиков В. А.,
доктор техн. наук, профессор,
генеральный директор Проекта МАКСМ
Пушкарский С. В.,
канд. техн. наук, старший научный сотрудник
Черкас С. В.,
канд. техн. наук, доктор военных наук
НИИ КС им. А. А. Максимова — филиал
ФГУП ГКНПЦ им. М. В. Хруничева*