

# Безопасность хранения и передачи медицинских (персональных) данных при многостороннем обмене медицинской информацией по программе «Международная космическая станция»

© А.П. Шуленин

© А.В. Скороходов

© Е.В. Кантемирова

Федеральное Государственное Бюджетное Учреждение ГНЦ РФ – ИМБП РАН  
Москва

ashulenin@imbp.ru

raido@imbp.ru

katarina@imbp.ru

© В.И. Почуев

© Л.М. Симаева

Федеральное Государственное Бюджетное Учреждение

«НИИ ЦПК имени Ю.А. Гагарина»

Звездный городок

l.simaeva@gctc.ru

## Аннотация

Представлены итоги работы Международной рабочей группы по медицинской информатике и технологиям при Многостороннем Совете по медицинским операциям Международной космической станции по созданию Многостороннего хранилища медицинских данных. Особое внимание при этом было уделено вопросам безопасности хранения и передачи медицинских (персональных) данных при соблюдении требований законодательства стран-партнеров по программе Международной космической станции.

## 1. Введение

Международная рабочая группа по медицинской информатике и технологиям (Medical Informatics and Technology Working group - MIT WG) при Многостороннем Совете по медицинским операциям МКС (Multilateral Medical Operations Panel - MMOP) была создана с целью разработки стратегии и технической реализации задач по передаче, хранению и обработке медицинской информации по экипажам Международной космической станции (МКС). Одним из итогов работы группы должно быть разработанное и функционирующее Многосто-

роннее хранилище медицинских данных (ISS Multilateral Medical Repository – IMMR).

Группа активно работает с 2005 года, членами MIT WG являются специалисты по медицинской информатике, представляющие космические агентства – партнеры по МКС: Роскосмос (Россия), NASA (США), ESA (Европа), CSA (Канада), JAXA (Япония).

Совершенствование технологии информационно-медицинского обеспечения полетов, сбор и обработка данных научных экспериментов, применение современной технологии обмена данных по компьютерным сетям дает значительный эффект в повышении уровня информационно-технического обеспечения медико-биологических аспектов космического полета, а также, при необходимости, в оказании лечебно-консультативной помощи экипажам орбитальных станций и других пилотируемых объектов в рамках программы МКС. Этому способствует правильно организованное медико-биологическое обеспечение, частью которого является и информационное сопровождение на основе современных компьютерных технологий сбора медицинской полетной информации и оперативного обмена медико-биологической информацией партнерами по МКС.

## 2. Разработка Многостороннего хранилища медицинских данных

Укрупненная схема взаимодействия медицинских организаций партнеров по МКС представлена на рис.1.

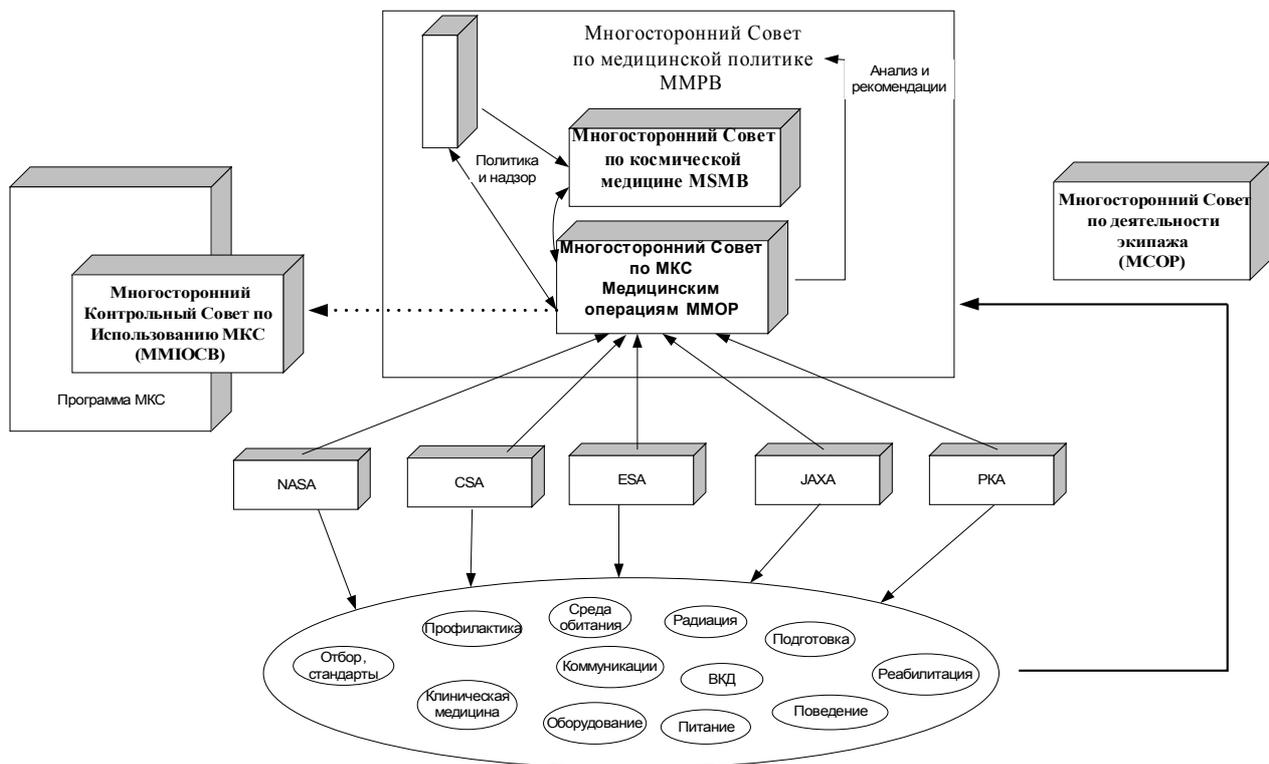


Рис. 1. Укрупненная схема взаимодействия медицинских организаций партнеров по МКС

Многосторонний Совет по Медицинским Операциям по программе МКС) руководит разработкой медицинских стандартов отбора и периодической сертификации всех членов экипажей МКС и участников КП.

ММОР и MSMB (Multilateral Space Medicine Board - Многосторонняя Комиссия по Космической Медицине) рассматривают и выносят решение по стандартам. Комиссия MSMB имеет право проводить медицинскую сертификацию членов экипажей МКС и экспедиций посещения. ММОР и MSMB работают на принципах консенсуса.

MMPB (Multilateral Medical Policy Board - Многосторонняя комиссия по вопросам медицинской политики) является высшим органом медицинского управления, который осуществляет контроль над охраной здоровья экипажа, а также организует обсуждение спорных вопросов совместно с MSMB и ММОР.

MCOP (Multilateral Crew Operations Panel - Многосторонняя комиссия по операциям экипажа) получает решения и заключения от MSMB.

MMIOCB (Multilateral Management Integration Operation Control Board - Многосторонняя комиссия по интеграции полета и операциям) получает требования и рекомендации от ММОР.

В процессе разработки IMMR специалисты группы изучили:

- руководящие документы, регламентирующие многосторонний обмен медицинской информацией по программе МКС [2, 3, 4, 11, 12, 19];
- информационные потоки медицинской информации в ходе подготовки к полету, управления полетом и послеполетной реабилитации экипажей [15];
- состав медицинской информации, предназначенной для многостороннего обмена [11];

- условия безопасного хранения и передачи медицинских (персональных) данных космонавтов и астронавтов при многостороннем обмене медицинской информацией [5];
- законодательную базу по работе с персональной информацией [18, 20, 21, 22];
- технические возможности партнёров.

Руководящие и нормативные документы определяют необходимость многостороннего обмена медицинской информацией по программе МКС, но не определяют стандарты по составу информации при медицинских исследованиях, стандарты обмена медицинской информацией между партнерами, стандарты по содержанию документов, подлежащих обмену по программе МКС.

По результатам проведенных исследований специалисты группы разработали пакет документов разного уровня ответственности (NASA, ММОР, MIT WG), регламентирующих процесс сбора, накопления и надежно защищенного обмена медицинскими данными между партнерами по МКС, позволяющий формализовать и юридически обосновать обмен медицинскими данными между партнерами по МКС.

Структура, индексация и взаимосвязь международных документов по обмену медицинскими данными представлены на рис. 2.

100 - MDS Security Policy (Политика в области безопасности обмена медицинскими данными). Содержит подписи ММОР, определяет основные категории данных и безопасности.

200 - MDS MaP (Medical Data Sharing Management Plan) (План управления обменом медицинскими дан-

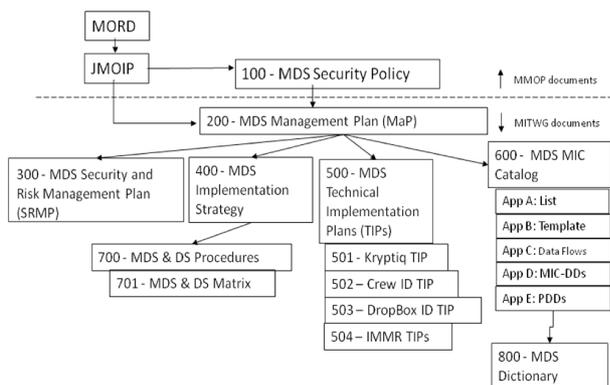


Рис. 2 Структура, индексация и взаимосвязь международных документов по обмену медицинскими данными

ными). Обеспечивает краткий обзор процесса обмена данными.

300 - MDS SRMP (Data Sharing Security and Risk Management Plan). March 24, 2006 (План управления безопасностью и риском обмена медицинскими данными). Обеспечивает краткий обзор многостороннего процесса безопасности. Объясняет различие между уменьшением риска и безопасностью. Должен быть заполнен каждым медицинским "юридическим лицом".

400 - MDS Implementation Strategy. (Стратегия Выполнения MDS).

500 - MDS Technical Implementation Plans. (MDS Технические Планы Выполнения). Обеспечивает детали для развития и испытания каждой технологии, метод или инструмент, который исследуется, обеспечивают план выполнения одобренных технологий.

600 - MIC Catalog. (Каталог МИКов, Прил.А – Список. Прил.В – Шаблон описания данных. Прил.С – Схемы потоков данных. Прил.Д – Описание данных в хранилище. Прил.Е – Описание данных партнеров).

700 - MDS&DS Procedures. (Процедуры MDS&DS). Список всех одобренных процедур обмена данных между Партнерами.

701 - MDS&DS Matrix. (Матрица MDS&DS). Список всех МИКов, которые были согласованы для обмена данными между Партнерами для любого экипажа.

800 - MDS Data Dictionary. (Словарь Данных MDS). Список элементов данных, подлежащих обмену.

Разработка документов базируется на основных Законах США и РФ – Закон о неприкосновенности частной жизни «Закон США о Приватности, 1974 года» [14], Российский Федеральный закон № 152-ФЗ «О персональных данных» от 27 июля 2006 г. [21], дополнительный Закон № 261-ФЗ РФ «О внесении изменений в Федеральный закон "О персональных данных" от 25 июля 2011 г. 1[22], а также соответствующих Законах других стран – партнеров по программе МКС.

Анализ требований руководящих документов, регламентирующих многосторонний обмен медицинской информацией по программе МКС и анализ существующих потоков медицинской информации в ходе подготовки к полету, управления полетом и послеполетной реабилитации экипажей по программе МКС позволили определить

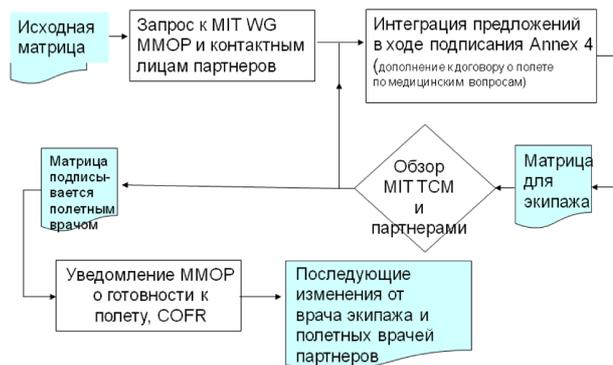


Рис. 3 Процесс формирования и согласования MATRIX

необходимый и достаточный состав медицинской информации, предназначенной для многостороннего обмена и принятия медицинских решений.

Разработана специальная Матрица (Matrix) [7, 8], позволяющая подробно описать каждую единицу информации (Medical Information Communiqués - MIC), подлежащую хранению и распределению. Информация в Матрице описывается метаданными, содержащими информацию о типе данных, фазе их сбора и/или использования, возможностях доступа, технологии защиты и передачи, ссылки на нормативные документы и пр.

Процесс формирования и согласования MATRIX многоэтапный и четко организован (рис. 3).

С использованием данной Матрицы разработана концепция IMMR.

IMMR предназначено для:

- хранения и накопления медицинских данных на всех членов экипажа по всем этапам подготовки, полета и реабилитации;
- информационного обеспечения Группы медицинского управления космическим полетом;
- поддержки принятия медицинских решений специалистами и руководством в ходе подготовки к полету, полета и этапа послеполетной реабилитации;
- накопления данных для анализа и совершенствования медицинского обеспечения космических полетов;
- формирования итогового отчета по полету;
- проведения научно-исследовательских работ, написания научных статей, диссертаций.

Определены следующие этапы разработки IMMR:

- 1 этап - создание версии IMMR, включающей базы данных и файловые системы для начала ее эксплуатации.
- 2 этап - создание единой базы данных с возможностями обращения к детальным данным средствами СУБД IMMR.
- 3 этап - создание программных средств анализа данных.

Первая очередь IMMR – официального многостороннего хранилища медицинских данных членов экипажа и соответствующих полетных данных, необходимых для проведения медицинских

операций и поддержки принятия решений, запущена в эксплуатацию на основе технологии Microsoft SharePoint, активно используемой партнёрами в NASA для организации совместной работы с данными [16, 17]. Доступ к системе осуществляется через стандартный веб-браузер. Это решение не требует дополнительных финансовых вложений от пользователей и обучения значительной части персонала, позволяет распределять доступ к данным, осуществлять поиск информации.

Для решения проблемы доступа должна быть решена задача структурированности хранилища информации:

- оперативное хранилище (информация используется в практической деятельности ежедневно);
- долговременное хранилище (информация используется для эпизодического просмотра, исторического обзора, ретроспективного научного поиска.)

К вопросу об объеме данных относятся и архивация документов. В реальной деятельности в ЦУП-М и Центре Управления Полетами-Хьюстон (ЦУП-Х) часто возникает необходимость ретроспективного просмотра архивных медицинских данных космонавтов (астронавтов). Если в перспективе будет решен вопрос о долговременном хранении данных в IMMR, будут достигнуты соглашения о потенциальной интеллектуальной собственности на хранимую в IMMR информацию, то необходимо предъявить требования к электронному обмену данными для проведения таких операций.

Система IMMR содержит контент с разграниченным доступом [9]. Потребители информации собраны в группы и имеют различные права доступа к информации, определяемые их должностными обязанностями. Группы потребителей информации частично коррелируют с рабочими группами в рамках ММОР. Данные могут быть предоставлены как нескольким группам в совместное использование, так и эксклюзивно малому кругу лиц [17]. Для получения доступа к системе требуется пройти процедуру согласования со службами информационной безопасности NASA.

Система IMMR позволяет осуществлять контроль исполнения документов, учитывая не только доступ, но и организацию хранения электронных документов, подготовку проектов и шаблонов документов, автоматизацию процессов согласования, контроль и мониторинг исполнения поручений, отчеты о сроках и фактах ознакомления с документами и информацией [6].

Архитектура многостороннего хранилища медицинской информации на сегодняшний день представлена на рис. 4.



Рис. 4 Архитектура многостороннего хранилища медицинской информации

Предусмотрено 5 уровней хранения данных в электронном виде:

1. Первичная информация из лабораторий и с борта МКС.
2. Хранилища информации у партнеров по МКС – в Агентствах и их организациях.
3. Хранилища информации партнеров в отдельных репозиториях в составе IMMR - накопление информации в ходе подготовки конкретного экипажа, утвержденного на полет.
4. Хранилища информации по конкретному экипажу с момента старта (фоновые значения) и полетные данные.
5. Архив – хранение информации по всем экспедициям.

Предусмотрены режимы работы пользователей IMMR: для администратора IMMR или владельца данных – ввод, корректировка, просмотр, удаление; для партнеров - только режим просмотра по допуску.

Важную часть работы составила организация доступа к IMMR для российских партнеров. В рамках решения проблемы был изучен и реализован вариант использования в Институте медико-биологических проблем (ИМБП), Центре Управления Полетами-Москва (ЦУП-М) и Центре подготовки космонавтов (ЦПК) системы защищенного удаленного доступа к данным VPN (Virtual Private Network - виртуальная частная сеть), т.н. Remote Access VPN. Данная технология позволила создать защищенный канал между сегментом внутренней сети NASA где расположен сервер IMMR, и пользователем, работающим с репозиторием удаленно (вне контура Космического центра им. Джонсона).

Для обеспечения обратной связи для пользователей IMMR был разработан интерактивный сайт, позволяющий оценивать работу IMMR и вносить предложения по его усовершенствованию и развитию. Сайт работает на аппаратно-программной базе ИМБП-ЦУМОКО (Центр управления медицинским обеспечением комических объектов).

### 3. Проблема безопасности хранения и передачи медицинских (персональных) данных по экипажам МКС

Современный этап развития систем информатизации предъявляет новые требования к защите информации. Информация рассматривается как некий товар, который можно продать, либо удачно использовать в своих целях. Потеря информационных ресурсов (несанкционированный доступ, хищение, блокирование и т.п.) может привести владельца информации к моральному и финансовому ущербу, принятию неправильных решений, утрате своих позиций.

Выполнение многоцелевых работ на МКС определяет наличие международного обмена информационными ресурсами, создание новых и совершенствование существующих средств информатизации по МКС и, соответственно, адекватного совершенствования их системы защиты. Этот факт вносит определенные требования при эксплуатации средств информатизации с точки зрения защиты внутренних информационных ресурсов.

К организации обмена медицинской информацией определены следующие требования:

- дополетные, полетные и послеполетные оперативные и научные медицинские данные на всех членов экипажа собираются и используются согласно «Закону США о Приватности, 1974 года» [12, 13];
- медицинские организации партнеров по МКС будут иметь доступ к информации о здоровье члена экипажа и ко всей информации, которая может быть значима для здоровья экипажа в течение всех фаз подготовки и полета;
- запросы на информацию о здоровье экипажа от сторонних организаций будут координироваться представителем медицинского управления партнера, как определено ММОР;
- общедоступная публикация медицинской информации относительно любого члена экипажа полета будет сделана только с предшествующим одобрением члена экипажа в соответствии с условиями «Закона США о Приватности, 1974 года» [14];
- технология обмена медицинской информацией должна обеспечивать соблюдение требований законодательств всех партнеров по МКС к трансграничному обмену персональной медицинской информацией.

В ходе работ выявилось наличие различий в требованиях законодательных и нормативных документов партнеров по сохранению конфиденциальности медицинской информации, что не позволяет в настоящее время обеспечить прямой доступ к персональной медицинской информации космонавтов и астронавтов при отсутствии соглашения соответствующего уровня об обмене медицинскими данными.

Одним из основных документов, разработанных специалистами Рабочей группы по медицинской информатике (MIT WG) при Многостороннем совете по медицинским операциям (ММОР), стал документ “MMOP Multilateral Medical Data Sharing Principles” (“Принципы многостороннего обмена медицинскими данными”) [13].

В данном документе представлены основные принципы совместного пользования многосторонними данными, защиты и безопасности данных, которые должны применяться в отношении данных медицинских операций на МКС, подлежащих совместному использованию. Представленные принципы должны приниматься во внимание всеми лицами и организациями, которые генерируют, обрабатывают, обсуждают или документируют данные по медицинским операциям, предназначенные для совместного пользования.

#### 3.1.

##### Классификация медицинских данных по уровню защиты

Защита медицинских данных должна осуществляться согласно классификации конфиденциальности [13, 20, 21, 22].

Медицинские данные и данные о здоровье будут классифицироваться по наличию признака, по которому какая-либо часть этих данных может быть соотнесена с определенным человеком.

К идентификационным данным относятся все конфиденциальные (медицинские, психологические, родственные) данные, которые можно однозначно приписать конкретному члену экипажа.

К обобщенным и обезличенным данным относятся данные, которые невозможно приписать конкретному члену экипажа.

К открытой информации относятся данные, которые можно без оговорок передавать в другие агентства.

При использовании в одном документе данных разного уровня защиты, устанавливается уровень защиты, соответствующий самому защищенному элементу.

Уровни защиты для различных типов данных представлены в Таблице 1.

Конфиденциальные данные должны иметь самый высокий уровень защиты на всех этапах манипуляций с ними.

Засекреченные данные должны быть защищены от публичного доступа и несанкционированного оглашения.

Несекретные данные не будут иметь особой защиты.

Данные, представляющие собой интеллектуальную собственность, должны рассматриваться как защищенные, если только они не содержат идентификационных данных по медицинским операциям, в противном случае они рассматриваются как конфиденциальные данные.

Таблица 1:

	Конфиденциальные	Защищённые	Незащищённые
Идентификационные	X		
Обобщённые или обезличенные		X	
Открытые			X
Интеллектуальная собственность:	X	X	

Кроме того, обсуждение конфиденциальных или защищённых данных любым комитетом, комиссией или группой по медицинским операциям должно классифицироваться таким же образом, включая все вербальные коммуникации и письменные отчеты, протоколы, замечания, но не ограничиваясь ими.

Разрабатываемая политика защиты медицинской информации при многостороннем обмене предлагается в документе “Data Sharing Security and Risk Management Plan” (DS SRMP) [1], разрабатываемым также MIT WG. Этот документ будет включать административные, физические, и технические меры безопасности, чтобы защитить частные (личные) и секретные данные от неправомерного раскрытия, разрушения, или модификации во время сбора, обработки, передачи или хранения.

### 3.2. Защита медицинских данных

После тщательного изучения соответствующих законов РФ и указаний NASA, распространяющихся на конфиденциальную информацию, к которой относится и персональная медицинская информация, было принято решение о необходимости обезличивания медицинской информации о космонавтах и астронавтах, участниках международной программы МКС.

Было решено создать систему, в которой происходило бы присваивание каждому астронавту/космонавту уникального и постоянного идентификационного кода уже на стадии принятия его в отряд астронавтов/космонавтов. Для реализации этой задачи была реализована методика, в которой личные данные заменяются на уникальный идентификатор “ID”. Также был составлен математический алгоритм генерации уникального идентификатора, на базе которого по стандартной схеме “клиент-сервер” была реализована Система “ID Code”. Используется два алгоритма ограничения доступа к серверу. Первый основан на списке разрешенных IP-адресов. Второй, который подключается после проверки валидности IP-адреса, использует стандартную пару «идентификатор учётной записи - пароль». Доступ к серверу возможен только по VPN.

Были выбраны, также, методы и процедуры обмена медицинскими данными между международными партнерами вне IMMR. Выбор основывался как на требованиях к безопасному обмену данными, так и на практике конкретных агентств, участвующих в программе. Учитывались особен-

ности местного законодательства и многолетняя практика использования тех или иных систем шифрования, например. Использование привычных технологий позволило «понизить» психологический барьер персонала, обучающегося работе с новой системой. Сочетание же различных методов, не всегда оптимальных, позволило учесть государственные нормативные требования по шифрованию данных. В результате, в обмене медицинской информацией задействованы следующие технологии и регламенты: Kryptiq, PGP, Secure FAX, Drop Box, Hand Delivery, Face-to-Face Verbal Exchanges, Electronic Voice Exchanges, SharePoint. IMMR стал одной из технологий обмена данными между партнерами.

### 3.3. Необходимость учёта международных, национальных и ведомственных нормативных документов

При работе с медицинскими данными должны соблюдаться требования политики безопасности, принятые в стране члена экипажа или участника космического полета. В каждой стране существуют свои законы, которые накладывают дополнительные требования к работе внутри страны.

В ходе исследований специалистами MIT WG выявлены следующие проблемы:

- несоответствие классификации уровней закрытости информации у партнеров по МКС;
- нерешенность вопросов использования криптографических средств при обмене медицинской информацией между партнерами по МКС;
- отсутствие юридических основ совместного использования данных партнерами по МКС.

Каждый партнер по МКС при работе с медицинскими данными должен соблюдать требования Законодательства своей страны, при этом тщательно отслеживая, что разрешено межправительственными договорами по данному вопросу.

Исследование проблемы безопасности хранения и передачи медицинских (персональных) данных при многостороннем обмене медицинской информацией по программе МКС проводилось с учетом требований Директивы Многосторонней комиссии по вопросам медицинских стратегий «Стратегия защиты медицинских данных в рамках программы МКС» («ISS Medical Data Security Policy») № 03 ММОР от 11 мая 2007 года.

Руководящие органы по медицинским операциям МКС, которые обеспечивают здоровье и безопасность экипажа МКС до полета, в течение полета и после полета, должны обеспечить безопасность медицинских данных и личных данных экипажа, как это определено в документе «Совместный план осуществления медицинского обеспечения МКС» (JMOIP, редакция октябрь 2007 года, раздел 12) [2].

В 1981 году Совет Европы принял Конвенцию «О защите личности в связи с автоматической обработкой персональных данных». В настоящее

время вопросы защиты персональных данных детально регламентируются директивами Европарламента и Совета Европейского Союза. Это Директивы № 95/46/ЕС и № 2002/58/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных» [18], Директива № 97/66/ЕС Европейского парламента и Совета Европейского Союза от 15 декабря 1997 года, касающаяся использования персональных данных и защиты неприкосновенности частной жизни в сфере телекоммуникаций и другие документы.

25 ноября 2005 г. Государственная Дума РФ ратифицировала данную Конвенцию (ФЗ от 19.12.2005 № 160\_ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматической обработке персональных данных»), возложив на Федеральные и муниципальные органы обязательства по приведению в соответствие с нормами европейского законодательства деятельности в области защиты прав субъектов персональных данных. Первым шагом в реализации взятых обязательств стало принятие Федерального закона № 152-ФЗ «О персональных данных» от 27 июля 2006 г. [21]. Закон вступил в силу в январе 2007 года. По результатам внедрения закона был издан дополнительный Закон № 261-ФЗ РФ «О внесении изменений в Федеральный закон "О персональных данных" от 25 июля 2011 года [22].

Этими законами впервые декларируются права субъекта персональных данных на его согласие на обработку его персональных данных. Под персональными данными понимается информация, относящаяся к определенному лицу, или информация, на основании которой определяется физическое лицо.

В соответствии со статьёй 10 Федерального закона №152\_ФЗ от 27 июля 2006 года медицинская информация отнесена к специальным категориям персональных данных.

Применительно к медицинским данным есть две статьи, позволяющие обработку медицинских данных, если она проводится лицом, профессионально занимающимся медицинской деятельностью.

В статье 6 Закона сказано - Согласие субъекта персональных данных на обработку его персональных данных не требуется в случаях:

- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

В статье 10 сказано - обработка специальных категорий персональных данных допускается в случаях, если:

- персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;
- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

Это можно рассматривать, как не запрещение на разработку международного хранилища медицинских данных по МКС и осуществление многостороннего обмена медицинской информацией по программе МКС.

На основании проведенных исследований по необходимости защиты информации и в соответствии с вышеприведенными классификационными признаками информационная система для многостороннего обмена медицинской информацией по программе МКС относится к 1 группе класса Д – «Многопользовательская АС, в которой одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС».

Эффективной защите конфиденциальной информации должна предшествовать разработка политики безопасности - комплекса превентивных мер против атак на информацию. Под политикой безопасности понимается совокупность документированных концептуальных решений, направленных на защиту информации и ассоциированных с ней ресурсов

#### **3.4. Трансграничная передача данных**

Трансграничная передача данных возможна лишь при выполнении определенных требований и условий в соответствии с Законом № 152-ФЗ «О персональных данных» [21]. Это означает, что разработку международного хранилища медицинских данных по МКС, осуществление многостороннего обмена медицинской информацией по программе МКС и обработку персональных данных можно осуществлять лишь с учётом требований данного закона (п.4, ст.10 «Обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ

сохранять врачебную тайну»; п.3, ст. 12 «Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных»).

С правовой точки зрения обеспечение адекватной защиты прав субъектов персональных данных предполагает соотношение правовых норм в сфере защиты персональных данных иностранного государства с правовыми нормами Российской Федерации или достаточность правового регулирования сферы защиты прав субъектов персональных данных исходя из особенностей конкретного иностранного государства.

Министерство связи и массовых коммуникаций РФ (Минкомсвязи) в своем письме № ДС\_П11\_2502 от 13.05.2009 определило «адекватную защиту» как защиту, при которой «обеспечивается уровень защищенности прав субъектов персональных данных не ниже, чем в Российской Федерации».

Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в некоторых случаях, в том числе в случаях исполнения договора, стороной которого является субъект персональных данных; защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

В Законе «О персональных данных» определено, что если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора (ст.4, п.4).

Одна из форм урегулирования трансграничной передачи персональных данных — наличие письменного соглашения, содержащего согласованные сторонами требования по защите персональных данных при их трансграничной передаче. Такие документы созданы в рамках рабочей группы ММОР по медицинской информатике и технологиям [1, 10, 13].

Законом Российской Федерации «О персональных данных» предусмотрено обязательное использование криптографических средств. Однако проблема состоит только в том, что мы не можем использовать российские криптографические средства для передачи данных партнерам, а предоставляемые партнерами средства должны быть сертифицированы в России. Кроме того, Законодательством России предусмотрено, что сервер ключей должен находиться в России.

## 4. Проблемы интеллектуальной собственности

Кроме проблемы защиты медико-биологической информации, остро стоит проблема защиты интеллектуальной собственности и потенциальной интеллектуальной собственности. Еще в 1992 году порядок охраны интеллектуальной собственности был изложен в «Соглашении между Российской Федерацией и Соединенными Штатами Америки о сотрудничестве в исследовании и использовании космического пространства в мирных целях» [19].

Соглашение регулирует вопросы распределения прав, интересов и отчислений между Сторонами. Каждая Сторона обеспечивает возможность для другой Стороны получать права на интеллектуальную собственность, распределенную в соответствии с Соглашением, путем приобретения этих прав от своих участников на контрактной основе или, если это будет необходимо, другими, предусмотренными законом средствами. Настоящее Соглашение не изменяет каким-либо иным образом и не наносит ущерб регулированию вопросов распределения между Стороной и ее участниками, которое определяется законами и практикой этой Стороны.

Стороны обеспечивают надлежащую и эффективную охрану интеллектуальной собственности, созданной или предоставленной в рамках упомянутого Соглашения и соглашений, заключенных в соответствии со статьей II Соглашения. Такие соглашения могут содержать различные положения об охране и распределении интеллектуальной собственности.

Юридические основы совместного использования партнерами по МКС медицинских данных по членам экипажей МКС в настоящее время отсутствуют. Законодательством регламентируются правоотношения по работе с интеллектуальной собственностью. Но интеллектуальной собственностью являются результаты обработки данных из многостороннего хранилища медицинских данных. Пока они не обработаны речь может идти только лишь о потенциальной интеллектуальной собственности, содержащейся в совокупности данных.

Первичные данные являются потенциальной интеллектуальной собственностью соответствующего космического агентства, а вопрос передачи всего комплекса первичной медицинской информации в настоящее время законодательствами стран партнеров по МКС не регламентирован и требует достижения договоренности.

На сегодняшний день в соответствии с документом [19] интеллектуальная собственность будет иметь максимально возможную защиту:

1) Права на публикацию и длительность действия первого права на публикацию будут защищаться по национальным законам и постановлениям в отношении владельца интеллектуальной собственности.

2) Права публикации данных, являющихся интеллектуальной собственностью, в каждом агентстве признаются всеми пользователями этих данных согласно заключенным между владельцем (владельцами) интеллектуальной собственности и пользователями договорами об обмене данными (Data Sharing Agreement).

3) Для персонала по медицинским операциям может быть предусмотрен быстрый доступ к данным научных исследований в период действия первого права на публикацию с разрешения владельца интеллектуальной собственности и исключительно для клинических целей.

4) Владелец интеллектуальной собственности может быть космическое агентство, компания, или частное лицо или они же в любой комбинации.

5) В связи с отсутствием заключения об уровне защиты персональных данных в странах – партнерах по программе МКС передача первичной медицинской информации партнерам и для хранения в многостороннем хранилище в настоящее время не целесообразна до урегулирования правовых вопросов по интеллектуальной собственности и потенциальной интеллектуальной собственности.

## 5. Мета-анализ информации

Острые и хронические последствия воздействия факторов космического полета недостаточно изучены, и для проведения научных исследований доступна весьма ограниченная информация. Поэтому анализ связей между этими факторами и здоровьем астронавтов строится на максимально эффективном использовании всех доступных данных.

Эпидемиологические исследования любого из партнеров по МКС не имеют достаточной статистической значимости для выявления доказательной связи между имевшим место внешним воздействием и состоянием здоровья, поскольку такие события случаются нечасто и число испытуемых невелико. Российское Федеральное Космическое Агентство (РКА) может предоставить сведения по примерно 250 космонавтам, NASA может предоставить сведения по примерно 350 астронавтов США, Европейское, Канадское и Японское космические агентства имеют очень малое количество участников космических полетов, совершивших разные по длительности полёты в космос и получивших разный опыт.

Однако совместное пользование медицинскими данными может быть весьма проблематичным из-за того, что агентства защищают медицинскую информацию и документацию, поскольку они могут быть персонально идентифицированы. Группа исследуемых мала, и все они заметные персоны. Объединение данных в один пул, что предусматривает мета-анализ, позволяет комбинировать относительные показатели воздействий по агентствам, при этом целостность и анонимность данных сохраняются.

Мета-анализ имеет определенные преимущества по сравнению с другими традиционными методами. Он позволяет эффективно использовать дополнительную информацию от других космических агентств, что в свою очередь позволяет повысить статистическую значимость исследований. Требуется исключительно несоотносимая информация (данные, которые не могут быть приписаны кому-либо), и можно избежать требований совместного пользования соотносимыми данными. Кроме того, данная методика позволяет охарактеризовать разнородность оценок воздействий по агентствам и выявить причины этих различий.

Применение методики мета-анализа было одобрено комиссией ММОР.

В рамках деятельности рабочей группы разработана концепция мета-анализа медицинской информации и начата обработка информации в NASA и Роскосмосе. Проводится обсуждение проекта мета-анализа в части, касающейся мероприятий ММОР по совместному пользованию данными. Обсуждаются вопросы защиты интеллектуальной собственности партнеров в ходе анализа медицинской информации. В фокусе внимания находятся принципы защиты совместного пользования данными медицинскими специалистами и специалистами-исследователями (научное сообщество).

## 6. Разработка методики многостороннего обмена медицинской информацией по программе МКС

Реализация многостороннего обмена медицинской информацией по программе МКС в рамках Роскосмоса в электронном виде на сегодняшний день представлена на рис. 5.

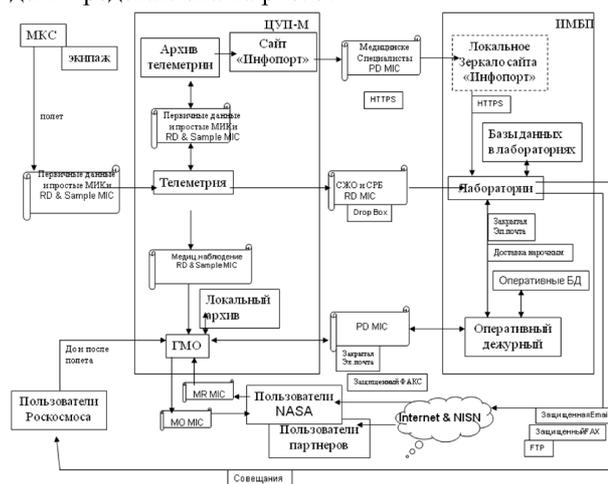


Рис. 5 Схема обмена медицинской информацией по программе МКС

Наличие разнородных информационных систем и технологий обмена медицинской информацией по программе МКС породило необходимость разработки специальной методики многостороннего

обмена медицинской информацией между партнерами по программе МКС.

Методика предназначена для руководителей и медицинских специалистов, осуществляющих медицинское обеспечение медико-биологической подготовки к полету, полета и этапа реабилитации.

Цель методики: методическое обеспечение руководителей и медицинских специалистов в процессе обмена медико-биологической информацией с партнерами по МКС для решения медицинских и организационных задач медицинского обеспечения подготовки к полету, полета и этапа реабилитации с соблюдением законов о защите персональных данных.

В основу методики многостороннего обмена медицинской информацией по программе МКС положен документ, разработанный специалистами MIT WG – “Medical Data Sharing and Data Security Procedures” [9].

## 7. Выводы

При работе с медицинскими данными МКС особое внимание было уделено требованиям политики безопасности, принятым в стране члена экипажа или участника космического полета. В каждой стране существуют свои законы, которые устанавливают дополнительные требования к работе внутри страны.

Несоответствие уровней закрытости информации у разных партнеров является сложной проблемой, так как нельзя изменить законодательство стран-партнеров, единственно, что можно сделать – найти соответствия между уровнями закрытости информации, определенными Законодательствами разных стран. Эта работа и проводится MIT WG в настоящее время.

В связи с отсутствием заключения об уровне защиты персональных данных в странах-партнерах по программе МКС передача первичной медицинской информации партнерам и для хранения в многостороннем хранилище в настоящее время не целесообразна до урегулирования правовых вопросов по интеллектуальной собственности и потенциальной интеллектуальной собственности.

## 8. Литература

[1] Data Sharing Security and Risk Management Plan (MDS SRMP). March 24, 2006, MIT WG 300

[2] International Space Station Joint Medical Operations Implementation Plan (ISS JMOIP), SSP 50480

[3] International Space Station Medical Operations Requirements Document (ISS MORD). Revision C. Incorporates DCN 007. February 2006

[4] ISS Medical Operations Data and Communication Concepts and Requirements, JSC-28289

[5] JMI 1382.5B, Maintaining the Privacy of Biomedical Research Data (JMI 1382.5B)

[6] Johnson-Throop, Kathy “IT Challenges for Space Medicine”, August 16, 2010 [http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20100033731\\_2010036785.pdf](http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20100033731_2010036785.pdf)

[7] Johnson-Throop, Kathy A.; Vowell, C. W.; Smith, Byron; Darcy, Jeannette “MDS MIC Catalog Inputs”, October 23, 2006 [http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20070029279\\_2007025859.pdf](http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20070029279_2007025859.pdf)

[8] MDS & DS Matrix, MIT WG 701

[9] Medical Data Sharing and Data Security Procedures (MDS & DS Procedures), NASA, ISS Program, JSC. Draft August 06, 2008. MITWG 1006

[10] Medical Data Sharing Management Plan (MaP), MIT WG 200 (План управления обменом медицинскими данными)

[11] Medical Evaluation Documents (MED), SSP 50667

[12] Medical Requirements Integration Documents (MRID), JSC 28913

[13] MMOP Multilateral Medical Data Sharing Principles. Date of MMOP approval MITWG Draft -18 June 2012

[14] Privacy Act of 1974. (Закон США о Приватности, 1974 года)

[15] Tao T Zhang, Gina G Aranzamendez, Susan S Rinkus, Yang Y Gong, Jamie J Rukab, Kathy Johnson-Throop, Jane T J Malin, Jiajie J Zhang “An information flow analysis of a distributed information system for space medical support”, 2004 Stud Health Technol Inform 107(Pt 2):992-6

[16] Vowell, C. W.; Johnson-Throop, Kathy; Smith, Bryon; Darcy, Jeannette “IMMR Phase 1 Prototyping Plan Inputs”, October 23, 2006 [http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20070029989\\_2007025858.pdf](http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20070029989_2007025858.pdf)

[17] Yang Gong, Tao Zhang, Jamie Rukab, Kathy Johnson-Throop, Jane Malin, Jiajie Zhang “Design and development of a search interface for an information gathering tool”, 2004 Stud Health Technol Inform 107(Pt 2):1471-5

[18] Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных.

[19] Соглашение между Российской Федерацией и Соединенными Штатами Америки о сотрудничестве в исследовании и использовании космического пространства в мирных целях, Вашингтон, 17 июня 1992 года.

[20] Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. № 188.

[21] 152-ФЗ «О персональных данных» от 27 июля 2006 г.

[22] 261-ФЗ РФ «О внесении изменений в  
Федеральный закон "О персональных данных " от  
25 июля 2011 г.

**Security storage and transmission  
of medical (personal) data  
for the multilateral exchange of medical information  
in frame of the program  
"The International Space Station"**

**Vladimir Pochuev, Lilia Simaeva, Anatoly Shulenin,  
Anton Skorokhodov, Ekaterina Kantemirova**

Herein presents results of the International Working Group on Medical Informatics and Technology at the Multilateral Medical Operations Council for the International Space Station to create a Multilateral storage of medical data. Particular attention was paid to the security of storage and transmission of medical (personal) data in accordance with the laws of countries-partners in the International Space Station program.