Киберсуверенитет в Здравоохранении и Медицине: Многоуровневая Модель Контроля и Подотчётности

Вагиф Мамедалиев
Институт Информационных Технологий, Баку, Азербайджан
vagifmammadaliyev@gmail.com

***Аннотация*— Процесс оказания медицинской помощи в здравоохранении 4.0 реализуется на основе быстрых интероперабельных систем с участием различных вендоров (поставщиков) и базируется на ИИ, IoMT, облачные технологии и большие объёмы данных. Хотя современные архитектуры, базирующиеся на указанных технологиях, расширяют клинические возможности, однако в условиях цифровой медицины они порождают новые вызовы, а традиционные взгляды относительно суверенитета медицинских данных оказываются недостаточно эффективными. В исследовании введено понятие киберсуверенитета в среде медицины 4.0, подразумевающее операционную способность, выходящую за рамки традиционного суверенитета данных и кибербезопасности, и интегрирующая управленческие, технические, интероперабельные и доказательные механизмы подотчётности в распределённых цифровых системах здравоохранения. Предложена четырёхуровневая модель поддержки киберсуверенитета в среде медицины 4.0. Модель связывает принципы киберсуверенитета с конкретными исполнимыми целями контроля и требованиями к доказательствам, охватывающим распространение и отзыв согласия, отслеживание источников данных, обязательства поставщиков, переносимость и непрерывную валидацию механизмов контроля.**

Keywords*— *киберсуверенитет; медицина 4.0; медицинские данные; многоуровневая модель поддержки контроля и подотчётности.

I. Введение

Медицина 4.0, использующая ИИ, IoT, большие данные и облачные платформы, усиливает зависимость здравоохранения от внешних многовендорных экосистем [1,2]. Эта зависимость расширяет поверхность атаки за счёт рисков интероперабельности, обмена данными с третьими сторонами и уязвимостей распределённых инфраструктур, а также усложняет контроль из-за ограниченной прозрачности потоков данных, их обработки и хранения [2]. Данные процессы формируют проблемы суверенитета, выходящие за рамки классической кибербезопасности, включая фрагментацию обязательств по соблюдению требований, ослабление фактического владения данными и снижение исполнимости механизмов управления в трансграничных сервисных цепочках. Совокупное воздействие этих факторов характеризуется как давление суверенитету (sovereignty pressure) - постоянная операционная и управленческая нагрузка, возлагаемая на медицинские организации в целях сохранения автономии, подотчётности и контроля в высокоскоростных взаимозависимых цифровых медицинских средах [2,3].

Преобладающие взгляды на суверенитет данных в здравоохранении часто сводят проблему к юридическому соответствию или локализации данных, однако облачно-ориентированная и многовендорная модель здравоохранения требует большего, чем правила, сосредоточенные исключительно на данных [2]. Суверенитет данных остаётся необходимой базовой предпосылкой, поскольку он определяет, кто обладает полномочиями в отношении медицинских данных и на каких условиях. Однако в условиях медицины 4.0 эти правила должны сохранять исполнимость по мере того, как данные проходят через интероперабельные устройства, внешние платформы и поддерживаемые ИИ контуры принятия решений [3]. Это смещает акцент проблемы с вопроса о том, где хранятся данные, к вопросу о том, может ли управление быть реализовано сквозным образом — на уровне механизмов идентификации и управления доступом, интерфейсов интероперабельности, платформенных зависимостей и механизмов подтверждения соответствия, формирующих доказательственную базу. Киберсуверенитет в медицине определяется как операционная способность, интегрирующая управление, безопасность, интероперабельность и операционный контроль для поддержания исполнимой подотчётности в распределённых цифровых инфраструктурах здравоохранения [2,3].

Предлагается многоуровневая модель, структурирующая киберсуверенитет в медицине в виде четырёх взаимодействующих управленческих слоёв — взаимодействия, данных, платформы и подтверждения соответствия (assurance) — с целью поддержки ориентированной на готовность оценки в многовендорных экосистемах здравоохранения [4]. На основе данной модели в качестве направления будущих исследований обозначена разработка Индекса медицинского киберсуверенитета (Medical Cyber Sovereignty Index),

DOI: 10.25045/cyber.gov.2026.52

предназначенного для трансформации слоистой модели в измеримые индикаторы и сравнительные оценки [4].

Настоящее исследование сосредоточено на концептуальной операционализации и демонстрации принципа работоспособности (proof-of-concept), а не на масштабной эмпирической валидации, тестировании чувствительности или разработке предписывающих рекомендаций по внедрению. Под операционализацией в данной статье понимается перевод общей идеи суверенитета в конкретные требования, механизмы контроля и показатели, которые можно применять на практике. Для иллюстрации того, как цели каждого слоя могут быть привязаны к правовым и институциональным основаниям, приводится юрисдикционное картирование на примере Азербайджана.

В отличие от существующих работ, которые, как правило, рассматривают суверенитет данных, цифровой суверенитет, кибербезопасность или платформенное управление по отдельности, в настоящем исследовании предлагается их интеграция в единую операционную рамку для условий Медицины 4.0. Научная новизна работы состоит в следующем. Во-первых, уточняется и адаптируется к сфере цифрового здравоохранения понятие медицинского киберсуверенитета как исполнимой организационно-технической способности сохранять контроль и подотчётность в распределённых многовендорных экосистемах. Во-вторых, предлагается авторская четырёхуровневая модель медицинского киберсуверенитета, включающая уровни взаимодействия, данных, платформы и подтверждения соответствия (assurance), что позволяет перевести обсуждение суверенитета из нормативно-декларативной плоскости в плоскость исполнимых механизмов контроля и доказательств. В-третьих, модель связывается с логикой оценки готовности и задаёт концептуальную основу для будущего Индекса медицинского киберсуверенитета. В-четвёртых, в качестве proof-of-concept показано, как цели уровней могут быть соотнесены с правовыми и институциональными основаниями на примере Азербайджана. Таким образом, статья не претендует на создание уже валидированного измерительного инструмента, а вносит вклад в виде концептуальной рамки.

II. Концептуальные предпосылки

A. Суверенитет в управлении медицинскими данными

Суверенитет данных в цифровом здравоохранении означает наличие полномочий и практического контроля над доступом к медицинским данным, их использованием и управлением ими, таким образом, чтобы решения о сборе, передаче, повторном использовании и вторичных целях оставались регулируемыми правами и мандатами законных обладателей данных [2,3]. В условиях цифрового здравоохранения суверенитет часто рассматривается через две взаимодополняющие, но порой конкурирующие ориентации [5,6]. Индивидуальный (персональный) суверенитет данных акцентирует личную субъектность, право пациента обладать, разрешать, ограничивать и отзывать согласие на использование своей медицинской информации [6,7]. Коллективный суверенитет данных подчёркивает легитимное институциональное владение и управленческую ответственность, при которых системы здравоохранения управляют данными для обеспечения непрерывности медицинской помощи, планирования в сфере общественного здравоохранения, мониторинга безопасности и выполнения обязательств по соблюдению нормативных требований [3,7]. Напряжённость между этими подходами становится очевидной, когда пациент-ориентированные механизмы контроля ограничивают агрегацию и повторное использование данных, необходимые для достижения более широких общественно-медицинских результатов, тогда как институционально-ориентированные модели рискуют ослабить индивидуальную автономию, если управление не является прозрачным, оспариваемым и исполнимым [6,7].

Однако важно рассматривать суверенитет данных как необходимую базовую предпосылку, а не как исчерпывающее решение для Медицины 4.0 [2,3]. Суверенитет данных преимущественно отвечает на вопрос, ориентированный на данные, а именно — кто обладает полномочиями в отношении медицинских данных и по каким правилам. Однако Медицина 4.0 вводит требование системно-ориентированного характера: эти правила должны оставаться исполнимыми по мере перемещения данных через интероперабельные устройства, сторонние платформы и поддерживаемые ИИ контуры принятия решений [2,8]. В экосистемах IoMT и многооблачных средах данные могут трансформироваться, агрегироваться, выводиться посредством аналитических моделей и реплицироваться между сервисами, которые не полностью наблюдаемы для исходной организации или пациента, что создаёт непрозрачность в отношении происхождения данных, их хранения и подотчётности [1,2]. В результате классические дискуссии о соотношении индивидуального и коллективного контроля усложняются тремя практическими факторами: распределённое хранение и обработка (distributed custody), при котором несколько вендоров обрабатывают или хранят медицинские данные на разных этапах; непрозрачность конвейера обработки (pipeline opacity), когда полный путь трансформаций данных и их последующего использования трудно поддаётся аудиту; и фрагментированность полномочий (fragmented authority), когда договорные, технические и юрисдикционные границы ограничивают механизмы принуждения даже при чётко сформулированных политиках [2,8,9].

Данный сдвиг объясняет, почему высокоуровневые принципы суверенитета, часто формулируемые как нормативные обязательства в отношении согласия, справедливости, распределения выгод и общественного контроля, могут быть трудны для операционализации в средах, поддерживаемых ИИ [10,11]. Сложность заключается не только в определении «надлежащего использования», но и во внедрении проверяемых механизмов, обеспечивающих реализацию управления со скоростью и в масштабах медицины 4.0 [12]. На практике операционализация требует исполнимых механизмов контроля, таких как детализированное управление

доступом и ограничение по цели использования, аудируемые процедуры предоставления и отзыва согласия, прослеживаемость происхождения данных и механизмы подотчётности, сохраняющие юридическую и операционную силу даже в случаях обработки данных внешними сервисами [2,13]. Эти требования обусловливают переход от одного лишь суверенитета данных к более широкой управленческой парадигме (структуре) — медицинскому киберсуверенитету, который явно включает инфраструктурные, идентификационные, интероперабельные и механизмы подтверждения соответствия (assurance), необходимые для сохранения исполнимости суверенитета в распределённых цифровых операциях здравоохранения [2,3].

Б. Киберсуверенитет в платформенных и облачно-ориентированных системах здравоохранения

Цифровой суверенитет часто используется как обобщающий термин для обозначения сохранения стратегического контроля над цифровыми возможностями, инфраструктурой и механизмами принуждения к соблюдению правил [3,4,14]. В контексте здравоохранения эта широкая идея операционализируется как медицинский киберсуверенитет, поскольку суверенные давления медицины 4.0 связаны не только с тем, где размещаются данные, но и с тем, сохраняется ли исполнимость управления в распределённых, многовендорных цифровых операциях здравоохранения [2,3]. Под операционализацией в данной статье понимается перевод общей идеи суверенитета в конкретные требования, механизмы контроля и показатели, которые можно применять на практике.

Медицинский киберсуверенитет определяется здесь как исполнимая способность медицинской организации осуществлять управление критически важными цифровыми активами здравоохранения по всей операционной цепочке (инфраструктура, управление идентификацией и доступом, потоки данных и поддерживаемые ИИ контуры принятия решений), даже если эти активы проходят через внешних поставщиков услуг и несколько правовых юрисдикций [2,3]. Новая парадигма акцентирует автономию, понимаемую как способность принимать и реализовывать решения относительно архитектур, вендоров, мест размещения и стратегий выхода/портируемости без чрезмерной зависимости [2,3], а также подотчётность, понимаемую как способность демонстрировать, проводить аудит и обеспечивать соблюдение политики и регулирования независимо от места обработки данных [2]. Данная интерпретация отличает медицинский киберсуверенитет от смежных понятий. Так, кибербезопасность сосредоточена на защите конфиденциальности, целостности и доступности от угроз [4], тогда как суверенитет данных фокусируется на полномочиях, правах и ограничениях в отношении доступа к данным и их использования [3]. Оба подхода необходимы, однако ни один из них по отдельности не гарантирует, что правила остаются исполнимыми и проверяемыми в условиях многооблачного здравоохранения [2]. Медицинский киберсуверенитет интегрирует эти измерения в управленческую способность, ориентированную на устойчивый операционный контроль, прослеживаемость и исполнимую подотчётность в многовендорной среде [4,14].

Облачные и многовендорные экосистемы усиливают суверенные вызовы, поскольку они превращают предоставление медицинских услуг в цепочку интероперабельных сервисов с неравномерной видимостью и фрагментированным контролем [2]. Требования интероперабельности расширяют уязвимость на границах интеграции, тогда как обработка третьими сторонами и распределённое хранение усложняют установление происхождения данных, их хранения и распределение ответственности [2,15]. В таких условиях соблюдение нормативных требований может фрагментироваться между вендорами и юрисдикциями, владение данными становится практически неоднозначным, когда они реплицируются, трансформируются или выводятся аналитически между сервисами, а механизмы принуждения к соблюдению управления ослабевают, если договорные, технические или юрисдикционные ограничения препятствуют своевременному вмешательству [2,16]. Надзор дополнительно осложняется неоднородными базовыми уровнями безопасности, различиями в трактовке требований к локализации данных и ограниченными возможностями независимой валидации механизмов контроля поставщиков, особенно в многооблачных развертываниях, где операционные политики реализуются через специфичные для каждого провайдера механизмы [2,17].

Соответственно, подлинный суверенитет в облачно-ориентированном здравоохранении требует синхронизированной интеграции правового и организационного управления с технической исполнимостью [2]. Это включает чёткое распределение ролей и ответственности между поставщиками, исполнимые договорные и аудиторские права [18], а также технические механизмы, обеспечивающие сквозную операционализацию управления: policy-as-code [2,19], согласованное управление идентификацией [2], фиксацию происхождения и жизненного цикла данных [19], непрерывную валидацию механизмов контроля [2] и подотчётность при инцидентах. На практике многие организации опираются на инструменты видимости и автоматизации управления для приближения такой исполнимости, включая управление конфигурацией безопасности облачной среды (cloud security posture management), управление правами доступа к облачной инфраструктуре (cloud infrastructure entitlement management) и панели мониторинга соответствия требованиям [2,20], поскольку ручные аудиты и периодическая отчётность слишком медленны для темпов и сложности рабочих процессов Медицины 4.0 [2]. Однако эти инструменты следует рассматривать как вспомогательные механизмы, а не как достаточные гарантии, поскольку суверенитет в конечном итоге зависит от способности организации реализовывать

управленческие решения и доказывать, что механизмы контроля остаются эффективными на протяжении всей многовендорной сервисной цепочки [2].

III. Многоуровневая Модель Медицинского Киберсуверенитета в Медицине

Нами предлагается четырёхуровневая операционная модель медицинского киберсуверенитета в рамках парадигмы Медицины 4.0 (Рисунок 1). Данная модель представляет собой ориентированную на готовность архитектуру управления, адаптированную к многовендорным экосистемам, в которых исполнимость обеспечивается за счёт механизмов контроля, сохраняющих свою валидность по мере того, как данные, идентичности и процессы принятия решений проходят через интероперабельные системы, облачные сервисы и поддерживаемые ИИ конвейеры обработки. Несмотря на различие по масштабу и области охвата, уровни сознательно сконструированы как взаимозависимые: суверенитет не может быть реализован путём усиления одного уровня в изоляции, поскольку недостатки распространяются по всей цепочке. Для удобства изложения уровни обозначаются как L1 — Взаимодействие, L2 — Данные, L3 — Платформа и L4 — Подтверждение соответствия (Assurance).

A. Взаимодействие

L1 регулирует легитимный доступ и использование в точке оказания медицинской помощи посредством интеграции надёжной идентификации и подтверждения ролей с механизмом согласия, которое реализируется как исполнимый объект контроля, а не как простая зафиксированная предпочтительная установка. Дополнительно требуется обеспечивать прозрачность, видимую для человека, позволяя пациентам и клиницистам проверять, к каким данным осуществлялся доступ, с какими целями и через какие системы они проходили. Ключевые цели включают:

- Исполнимое согласие, распространяемое на последующие системы, с возможностью отзыва и временных ограничений полномочий.
- Подтверждение идентичности и ролей, при котором действия остаются атрибутируемыми и не подлежащими отказу от совершения во всех клинических, административных и управляемых поставщиками интерфейсах.
- Механизмы прозрачности, обеспечивающие возможность проверки путей доступа и принятия решений субъектами данных и их подотчётность медицинским командам, а не сокрытие в непрозрачных сервисных слоях.

Б. Данные

L2 регулирует жизненный цикл данных от сбора до повторного использования — включая приём, обработку, передачу, трансформацию и хранение — посредством исполнимых правил минимизации, ограничения по цели, допустимых преобразований и вторичного использования. Эти правила поддерживаются механизмами фиксации происхождения, обеспечения целостности и привязки политик. Ключевые цели включают:

- Обработку, ограниченную политикой и целью, которая последовательно сохраняется по мере прохождения данных через сервисы и их интеграции с другими наборами данных.
- Сквозную прослеживаемость происхождения и подотчётность, при которых каждая трансформация, аналитический вывод и раскрытие данных соотносятся с санкционированным основанием.
- Явное управление вторичным использованием, сохраняющее соответствие первоначальным правам и условиям.

Данный уровень также операционализирует этическое напряжение между индивидуальным и коллективным суверенитетом: одних лишь механизмов защиты индивидуальной конфиденциальности может быть недостаточно для обеспечения гарантий общественного здравоохранения, тогда как коллективное использование должно быть ограничено исполнимыми правилами, прозрачным управлением и подотчётным хранением данных.

L3 – Платформа

L3 операционализирует суверенитет в отношении устройств IoMT, пограничных шлюзов, облачных платформ и интероперабельных сред посредством обеспечения того, чтобы архитектурные и вендорные решения оставались явными, управляемыми и обратимыми. Решения о размещении и локализации рассматриваются как управленческие решения, договорные обязательства и ответственность поставщиков трансформируются в исполнимые технические механизмы контроля, а механизмы переносимости и стратегии выхода являются обязательными для снижения риска технологической зависимости. Ключевые цели включают:

- Интероперабельность под локальным управлением, при которой интеграция не приводит к скрытой передаче контроля над идентификацией, журналированием, принуждением к соблюдению политик или перемещением данных поставщикам.
- Операционная независимость от зависимости от одного провайдера, достигаемая посредством управляемых шлюзов, сегментации, стандартизированных интерфейсов и протестированных процедур переносимости/выхода.
- Устойчивость операций, обеспечивающая сохранение доступности и целостности при сбоях, включая распределённые модели управления доступом, механизмы обеспечения непрерывности и изоляцию инцидентов с учётом зависимостей.

L4 – Подтверждение соответствия (Assurance)

L4 выполняет функцию доказательного уровня, посредством которого суверенитет становится демонстрируемым и исполнимым на практике. В него включаются многоуровневое управление, аудитируемость (контролируемость) по замыслу, непрерывное поддержание соответствия требованиям и механизмы реагирования на инциденты — с чёткой подотчётностью за решения, сбои и причинённый вред. Ключевые цели включают:

- Аудируемые политики и обязательства поставщиков, обеспечивающие исполнимый надзор.
- Готовность к инцидентам, поддерживаемая чётко определёнными границами ответственности и прослеживаемыми записями решений между внутренними командами и внешними поставщиками.
- Надзор по принципу «этика по замыслу» (ethics-by-design), обеспечивающий адаптивность принципов суверенитета к юрисдикционным реалиям, динамике доверия и развивающимся клинико-ИИ практикам, а не сводящий их к периодическим формальным отчётным процедурам.

Взаимодействие слоев

Принципы суверенитета посредством данных уровней связываются с конкретными решениями в отношении субъектов, данных, платформ и механизмов подтверждения соответствия. Легитимные субъекты и их полномочия устанавливаются уровнем L1; исполнимость этих полномочий в процессе трансформации данных и их повторного использования обеспечивается уровнем L2; техническая основа и вендорные зависимости, которые могли бы подорвать эти полномочия, нейтрализуются на уровне L3; а доказательная база и механизмы подотчётности, необходимые для проверки соблюдения требований и реагирования на сбои управления, формируются уровнем L4. Данная взаимосвязанная структура предназначена для содействия практической оценке готовности, позволяя организациям выявлять вероятные сбои суверенитета в условиях медицины 4.0, а не рассматривать суверенитет как единичное абстрактное свойство «наличия защищённых систем» или «локализации данных». Поскольку каждый уровень определяет конкретные цели контроля и требования к доказательствам, модель может быть преобразована в измеримые индикаторы (например, исполнимость отзыва согласия, прослеживаемость происхождения данных, протестированная переносимость/выход, непрерывная валидация механизмов контроля). Это формирует концептуальную основу для будущего Индекса медицинского киберсуверенитета и для оценки готовности, привязанной к конкретной юрисдикции.

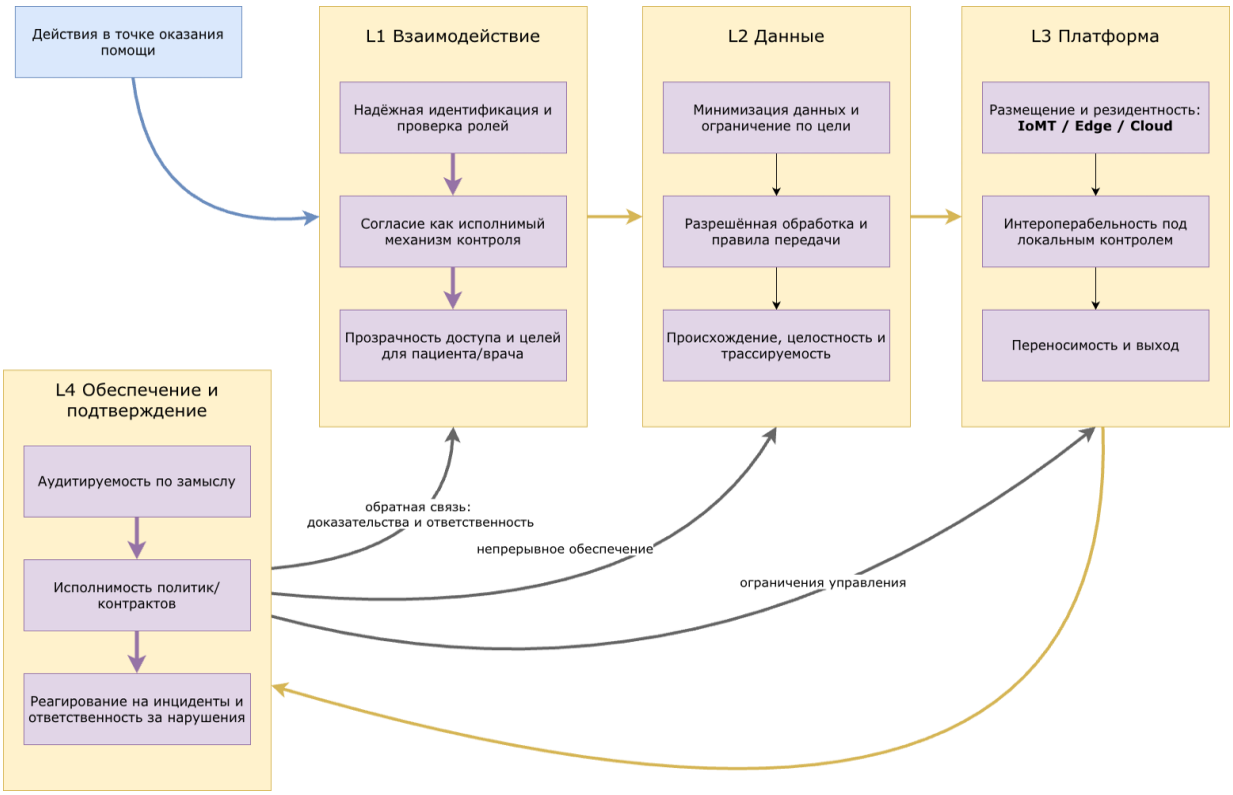

Рисунок 1. Четырёхуровневая операционная модель медицинского киберсуверенитета в медицине.

IV. Операционализация модели и иллюстрация на примере Азербайджана

Разработка количественно измеримых показателей для четырёхуровневой модели представляет собой следующий логичный шаг, поскольку принципы суверенитета и управления остаются абстрактными, пока они не преобразованы в наблюдаемые механизмы контроля, проверяемые доказательства и юрисдикционно-специфические обязательства. Практическая оценка суверенитета, таким образом, требует двух ключевых согласований: сопоставления целей каждого уровня с исполнимыми техническими и организационными механизмами контроля и привязки этих механизмов к правовым, институциональным и операционным реалиям соответствующей юрисдикции здравоохранения. В целях иллюстрации такой операционализации без чрезмерного акцентирования эмпирической валидации представлено доказательство концепции (proof-of-concept) на примере Азербайджана как одной из возможных юрисдикций.

Оценка готовности для L1 и L2 может быть привязана к требованиям Азербайджана в сфере персональных данных и конфиденциальности путём концептуализации согласия, авторизации и законной обработки как проверяемых свойств принуждения к соблюдению, а не абстрактных политических деклараций [22]. Нормативные положения, связывающие обработку с согласием и признающие отзыв согласия как значимый механизм контроля, могут быть операционализированы в кластеры индикаторов, включая:

- согласие, зафиксированное в форме, подлежащей машинному принуждению к исполнению
- отзыв согласия, распространяемый на все подключённые последующие системы
- решения о доступе, атрибутируемые конкретным ролям и идентичностям
- обеспечение понятной и применимой прозрачности для пациентов и клиницистов в отношении целей доступа и раскрытия данных

Национальный реестр информационных систем персональных данных Азербайджана обеспечивает дополнительную основу для измеримости на уровне L2: требования регистрации, декларирование объёма обработки и административная ответственность за использование незарегистрированных систем могут быть операционализированы как индикаторы институциональной подотчётности и готовности к законной обработке данных. Такие индикаторы смещают оценку от «заявленного соответствия» к демонстрируемому исполнению управления, включая прослеживаемость операций обработки и доказуемость обработки, ограниченной политиками, на протяжении всего жизненного цикла данных [23].

Для L3 измеримость в Азербайджане может опираться на государственные инициативы и регулирование критической информационной инфраструктуры, которые имплицитно формируют ожидания в отношении суверенного размещения, границ надзора и базовых обязательств по обеспечению безопасности в жизненно важных сферах, таких как здравоохранение. Оценка готовности должна подтверждать контроль над операционной плоскостью управления — включая принуждение к соблюдению идентификации, развёртывание политик, журналирование, управление ключами, сегментацию и механизмы выхода/переносимости, — а не ограничиваться простым перечислением используемых технологий или облачных провайдеров. Например, инициатива «Government Cloud» может служить основой для индикаторов, проверяющих, размещаются ли критически важные медицинские нагрузки и чувствительные данные в средах под внутренним надзором и реализуется ли операционное управление национальными или институциональными субъектами. Аналогичным образом, регулирование критической информационной инфраструктуры может задавать объективные критерии платформенного суверенитета, такие как исполнимые обязательства поставщиков, демонстрируемое соответствие базовым механизмам контроля и наличие доказательств того, что интероперабельность не приводит к скрытой передаче полномочий по принятию решений внешним вендорам [21].

В целом картирование на примере Азербайджана представлено как пример юрисдикционной операционализации, а не как валидированный национальный эталон. Оно демонстрирует, каким образом четырёхуровневая модель может быть преобразована в измеримые индикаторы готовности посредством привязки целей уровней к исполнимым обязательствам, наблюдаемым механизмам контроля и проверяемым доказательствам. Дальнейшие исследования должны формализовать таксономию индикаторов, определить шкалы оценки и логику агрегирования, а также оценить надёжность и чувствительность на уровне нескольких организаций и юрисдикций, чтобы обеспечить, что создаваемый индекс отражает готовность к обеспечению суверенитета, а не риторику формального соответствия требованиям.

Заключение

Медицина 4.0 усугубляет вызовы суверенитета, трансформируя клиническую помощь в быструю цепочку интероперабельных многовендорных сервисов, в которой управление должно сохранять исполнимость в условиях распределённого хранения и обработки, непрозрачных конвейеров и трансграничных зависимостей. В ответ на эту трансформацию медицинский киберсуверенитет представлен как операционная способность, различающаяся от суверенитета данных и кибербезопасности, но дополняющая их.

Предложена четырёхуровневая модель для структурирования исполнимого контроля и подотчётности на уровнях взаимодействия, управления жизненным циклом данных, управления платформами и зависимостями, а также подтверждения соответствия и

доказательной подотчётности. Модель обеспечивает практическую перспективу оценки готовности посредством установления связей между принципами суверенитета и конкретными решениями и механизмами контроля, охватывающими субъектов, данные, платформы и механизмы доказательства. При этом сбои суверенитета, как правило, возникают на границах уровней, а не внутри изолированных технических компонентов.

На примере Азербайджана показано, как цели уровней можно перевести в конкретные измеримые показатели с учётом правовой и институциональной базы страны. Основной акцент сделан на подтверждаемом управлении, а не на декларативных заявлениях. В дальнейшем планируется разработать систему показателей и методику оценки для Индекса медицинского киберсуверенитета и проверить их применимость в разных юрисдикциях.

Список литературы

[1] Centers for Disease Control and Prevention, “What is population health?,” [Online]. Available: https://archive.cdc.gov/www_cdc_gov/pophealthtraining/whatis.html.

[2] A. Muhammed and E. Blix, “Digital Sovereignty in a Multi-cloud Environment in the Health Sector,” Jun. 2025.

[3] InCountry, “Essentials and challenges of healthcare data sovereignty laws,” Oct. 28, 2024. [Online]. Available: https://incountry.com/blog/essentials-and-challenges-of-healthcare-data-sovereignty-laws.

[4] C. Maathuis and K. Cools, “Digital Sovereignty Control Framework for Military AI-based Cyber Security,” 2025, arXiv:2509.13072. [Online]. Available: https://arxiv.org/abs/2509.13072.

[5] P. Hummel, M. Braun, M. Tretter, and P. Dabrock, “Data sovereignty: A review,” Big Data & Society, vol. 8, no. 1, Jan. 2021, doi: 10.1177/2053951720982012.

[6] J. Piasecki and P. Y. Cheah, “Ownership of individual-level health data, data sharing, and data governance,” BMC Medical Ethics, vol. 23, no. 1, Oct. 2022, doi: 10.1186/s12910-022-00848-y.

[7] A. Cordes et al., “Title unavailable,” npj Digital Medicine, 2024, doi: 10.1038/s41746-024-01171-z.

[8] S. E. El-deep, A. A. Abohany, K. M. Sallam, and A. A. A. El-Mageed, “A comprehensive survey on impact of applying various technologies on the internet of medical things,” Artificial Intelligence Review, vol. 58, no. 3, Jan. 2025, doi: 10.1007/s10462-024-11063-z.

[9] U. Islam et al., “A hybrid fog-edge computing architecture for real-time health monitoring in IoMT systems with optimized latency and threat resilience,” Scientific Reports, vol. 15, no. 1, Jul. 2025, doi: 10.1038/s41598-025-09696-3.

[10] J. Morley et al., “Governing Data and Artificial Intelligence for Health Care: Developing an International Understanding,” JMIR Formative Research, vol. 6, no. 1, Jan. 2022, doi: 10.2196/31623.

[11] J. S. Winter, “AI in healthcare: data governance challenges,” Journal of Hospital Management and Health Policy, vol. 5, p. 8, Mar. 2020, doi: 10.21037/jhmhp-2020-ai-05.

[12] M. Hähnel, “Ethical challenges and solutions in AI-driven medical data management: a focus on distributed machine learning,” Discover Artificial Intelligence, vol. 5, no. 1, May 2025, doi: 10.1007/s44163-025-00266-0.

[13] F. Guitton, A. Oehmichen, É. Bossé, and Y. Guo, “Honest Computing: Achieving demonstrable data lineage and provenance for driving data and process-sensitive policies,” 2024, arXiv:2407.14390. [Online]. Available: https://arxiv.org/abs/2407.14390.

[14] Z. Kotulski et al., “Keeping Verticals’ Sovereignty During Application Migration in Continuum,” Journal of Network and Systems Management, vol. 32, no. 4, Jul. 2024, doi: 10.1007/s10922-024-09843-7.

[15] Z. Zandesh, “Privacy, Security, and Legal Issues in the Health Cloud: Structured Review for Taxonomy Development,” JMIR Formative Research, vol. 8, Feb. 2024, doi: 10.2196/38372.

[16] A. K. Polinati, “Hybrid Cloud Security: Balancing Performance, Cost, and Compliance in Multi-Cloud Deployments,” 2025, arXiv:2506.00426. [Online]. Available: https://arxiv.org/abs/2506.00426.

[17] D. Seth, M. Najana, and P. Ranjan, “Compliance and Regulatory Challenges in Cloud Computing: A Sector-Wise Analysis,” Jun. 2024, doi: 10.21428/e90189c8.68b5dea5.

[18] F. Conteh, “Artificial Intelligence and Applications,” Jan. 2024, doi: 10.5121/csit.2024.1401.

[19] N. K. M. Pulikonda, “Real-Time Clinical Data Governance Architecture: Financial Compliance-Inspired Model for HIPAA/HITECH Compliance,” Journal of Computer Science and Technology Studies, vol. 7, no. 4, p. 712, May 2025, doi: 10.32996/jcsts.2025.7.4.84.

[20] K. G. Boamah, “Cloud Security Posture Management: A Comprehensive Analysis of Automated Risk Identification and Mitigation in Multi-Cloud Environments,” International Journal of Research and Innovation in Social Science, vol. 9, no. 11, p. 4458, Dec. 2025, doi: 10.47772/ijriss.2025.91100349.

[21] Ministry of Digital Development and Transport of the Republic of Azerbaijan, “Government Cloud,” [Online]. Available: https://mincom.gov.az/en/projects/government-cloud.

[22] Azərbaycan Respublikası, “Fərdi məlumatlar haqqında” (О персональных данных), Azərbaycan Respublikasının Qanunu, 11 may 2010. [Online]. Available: https://e-qanun.az/framework/19675.

[23] Ministry of Digital Development and Transport of the Republic of Azerbaijan, “State Register of Personal Data Information Systems,” [Online]. Available: https://registry.pdp.az.

Cyber Sovereignty in Healthcare and Medicine: A Multilevel Model of Control And Accountability

Vagif Mammadaliyev
Institute of Information Technology, Baku, Azerbaijan

Abstract– The delivery of healthcare services in Healthcare 4.0 is implemented through fast, interoperable systems involving multiple vendors (providers) and is based on artificial intelligence (AI), the Internet of Medical Things (IoMT), cloud technologies, and large-scale data. While modern architectures built on these technologies expand clinical capabilities, in the context of digital medicine they also introduce new challenges, and traditional approaches to medical data sovereignty prove insufficiently effective. This study introduces the concept of cyber sovereignty within the Healthcare 4.0 environment, defined as an operational capability that extends beyond traditional notions of data sovereignty and cybersecurity, integrating governance, technical, interoperability, and evidence-based accountability mechanisms in distributed digital healthcare systems. A four-level model for supporting cyber sovereignty in Healthcare 4.0 is proposed. The model links cyber sovereignty principles with concrete, enforceable control objectives and evidence requirements, encompassing consent propagation and revocation, data provenance tracking, vendor obligations, portability, and continuous validation of control mechanisms.

Keywords– cyber sovereignty; Healthcare 4.0; medical data; multilevel model for control and accountability support.