
Аналитический рабочий доклад

Посольства данных и суверенная непрерывность Саудовской Аравии: сравнительная проверяемая модель

Аналитический рабочий доклад сопоставляет правовую защиту посольства данных, опыт сохранения реестров во время войны и катастроф и технологии криптографического распределения, а затем предлагает критерии испытаний до возможного применения в Саудовской Аравии.

Дата материала

18 октября 2026 г.

Автор

Safwan AlModhayan

Ключевые слова: посольство данных · суверенная непрерывность · цифровой суверенитет · пороговая криптография · непрерывность государственного управления · управление рисками

Аналитический рабочий доклад подготовлен на основе статьи автора и открытых источников, доступных на 18 октября 2026 года. Это не рецензированное исследование, не юридическое заключение и не отчет о проведенном испытании или фактических результатах государственного проекта.

isafwan.com/ru/research/data-embassies-sovereign-continuity/

Аннотация

В работе рассматривается суверенная непрерывность (Sovereign Continuity) и условия, при которых внешнее размещение государственных данных становится ее инструментом, а не удаленной резервной копией или новой зависимостью.

Отправная точка: непрерывность государства соединяет реестр, программное обеспечение, идентичность, подпись, связь и законное полномочие; одной целостности данных недостаточно для их применения или истинности.

Документальный сравнительный метод рассматривает соглашение Эстонии и Люксембурга как правовой случай, а Украину, Кашмир, Сирию, Судан и Шпицберген — как случаи разных отказов и восстановления. Сравнение связано с литературой об аварийном восстановлении, отказах по общей причине, разделении секрета, целостности записей и саудовских правилах трансграничной передачи и облачных вычислений. ^[1]_[16]

Результат — схема испытаний, а не результат эксперимента. Саудовскую модель следует оценивать по независимости точек отказа; способности выполнять определенные функции в пределах целевого времени восстановления (Recovery Time Objective, RTO) и целевой точки восстановления (Recovery Point Objective, RPO); законности полномочий; проверяемости цепочки происхождения (Provenance); соблюдению норм; сменяемости хоста, поставщика и алгоритма. Работа не утверждает, что внешнее размещение необходимо всякой функции или допустимо для каждой категории данных.

Вопрос и границы исследования

Главный вопрос: при каких правовых, технических и операционных условиях многоплощадочная схема, частично размещенная за пределами Королевства, может снизить риск утраты способности саудовского государства подтверждать права и выполнять конкретные суверенные функции при отказе площадок, сетей или административных полномочий?

Из него следуют четыре вопроса: что правовая защита добавляет к договору хостинга; какой минимум должен перемещаться вместе с данными, чтобы функция оставалась исполнимой; как распределить ключи и копии, не создавая

единоличной внешней власти; как проверить пользу и риск до применения чувствительных данных?

Работа не оценивает законность конкретного проекта: для этого нужны категория данных, цель обработки, рабочая архитектура, принимающие страны и решения компетентных органов. Она не дает количественной вероятности войны или прогноза финансового эффекта и не утверждает причинную связь между посольствами данных и стабильностью рынков.

Документальный метод и отбор случаев

По возможности используются первичные либо близкие к событию источники: официальный текст соглашения Эстонии и Люксембурга; государственные и судебные материалы об Украине и Кашмире; правозащитные и гуманитарные материалы о Сирии и Судане; документация Шпицбергена; саудовские нормы; оригинальные или нормативные материалы Шамира и NIST. Новости и заявления рассматриваются как ограниченные окна в событие и не подменяют независимую проверку.

Случаи отобраны по аналитической функции, а не как равнозначные. Эстония показывает правовой инструмент хостинга; Украина — сохранение критических реестров после удара по площадке; Кашмир и Сирия — влияние утраты записей на право; Судан — разрыв между сохранностью и связью; Шпицберген — восстановление возможности, а не только копии. ^{[1] [2] [3] [4] [5] [6] [7] [8] [9]}

Сравнение идет по шести измерениям: защищаемый актив, угроза, независимость площадки, восстановимость и исполнимость, полномочие дать команду на восстановление, границы доказательств. Метод не допускает статистического обобщения, но выявляет условия для гипотез и испытаний прототипа.

Операционные определения

Посольство данных (Data Embassy) здесь означает зарубежную площадку государственных данных и систем с особым правовым статусом, заданным межгосударственным соглашением; это не перенос территории и не автоматический дипломатический иммунитет. Суверенная непрерывность —

способность сохранять выбранные публичные функции исполнимыми и проверяемыми при серьезных нарушениях, оставляя конечное правовое решение и контроль государству.

Аварийное восстановление (Disaster Recovery) возвращает технический ресурс после сбоя; непрерывность государственного управления (Continuity of Government) сохраняет основные функции во время нарушения или возвращает их в допустимых пределах. Техническое восстановление может быть успешным, а публичный результат — провальным, если система вернулась позже срока, который выдерживает право или услуга.

Цепочка происхождения (Provenance) позволяет проследить источник данных, изменения и полномочие на них. Целостность данных (Integrity) выявляет несанкционированное изменение, но сама по себе не доказывает правильность первого ввода. Отказ по общей причине (Common-Mode Failure) одновременно выводит из строя резервные решения из-за общей зависимости; поэтому настоящее разнообразие важнее формального географического распределения.^[10]

Сравнение: случаи и выводы

Эстонский случай показывает: юридическую ценность создает не название, а текст, определяющий неприкосновенность площадки, доступ, связь, применимое право, спор, прекращение и передачу активов. Он подтверждает, что одной Венской конвенции недостаточно. Соглашение не превращает площадку в эстонскую землю, а создает ограниченную международно-правовую защиту.^[1]

Официальное украинское сообщение показывает, как заранее распределенные реестры и резервные ресурсы могут не дать физическому удару остановить критический реестр, но не является независимым аудитом каждой системы. Кашмир и Сирия показывают, что утрата документа ослабляет доказуемость права. Судан — что целый архив не обеспечивает услугу без связи, идентичности и платежных средств.^{[3] [4] [5] [6] [7]}

Шпицберген дает функциональную меру: сохранение доказало себя, когда образцы извлекли, вырастили, размножили и снова поместили в хранилище. По аналитической аналогии копия министерства не обеспечивает непрерывность,

пока нельзя запустить программы, проверить личность и подпись и законно использовать реестр. Семена и данные не отождествляются; аналогия показывает критерий функционального восстановления. ^[8]

Правовая рамка: конкретная защита, а не вакуум суверенитета

Соглашение Эстонии и Люксембурга защищает площадку от обыска, ареста и исполнения решений и требует согласия эстонского представителя на вход. В чрезвычайной ситуации согласие предполагается только для немедленной защиты от угрозы безопасности. Статья 6 рассматривает данные и системы как архив, защищает официальную связь и допускает шифрование. Статья 8 сохраняет международное право, право ЕС и применимое право Люксембурга и регулирует арбитраж. ^[1]

Статья 10 делает прекращение действительным через двадцать четыре месяца после уведомления и различает передачу активов уполномоченному представителю и случай, когда его нельзя определить: тогда активы защищаются и выдаются только законному представителю. Эти положения заранее решают судьбу архива при ухудшении отношений или споре о представительстве. ^[1]

В Саудовской Аравии трансграничная передача персональных данных обусловлена национальной безопасностью, жизненно важными интересами, необходимым минимумом, уровнем защиты, правами лиц и оценкой адекватности, гарантиями либо указанными исключениями. Международное соглашение — один из путей в процедуре компетентного органа, а не автоматическое разрешение. Требования к кибербезопасности облачных вычислений (Cloud Cybersecurity Controls, CCC) — рамка безопасности в своей сфере, а не замена нормам о данных, классификации и отраслевым условиям. ^[14] ^[15]

Техническая рамка: распределение данных и власти

Нужно различать аутентифицированное шифрование (Authenticated Encryption), кодирование с исправлением стираний (Erasure Coding) и пороговую криптографию (Threshold Cryptography). Первое защищает конфиденциальность и выявляет подмену, второе распределяет фрагменты для доступности содержимого, третье распределяет власть над ключами или операциями. Смешение технологий приписывает одному слою функции другого.

Разделение секрета Шамира (Shamir's Secret Sharing) дает пороговую гарантию: при корректной математической реализации порог восстанавливает секрет, меньшая группа не узнает о нем ничего. Схема «три из пяти» выдерживает потерю двух долей, но не доказывает доступность данных, законность команды или безопасность устройств. Нужны независимые хранители, защита и ротация долей, наблюдение и испытанная замена отсутствующего либо ненадежного хранителя. ^[11]

Многосторонние вычисления (Multi-Party Computation) и пороговые подписи (Threshold Signatures) вместе с аппаратными модулями безопасности (Hardware Security Modules, HSMs) могут выполнять операции без сборки полного ключа в одном месте. Но сложность протокола увеличивает нагрузку на аудит и реагирование. Мера качества — не новизна, а снижение конкретного риска при работоспособности в худших условиях.

Целостность записи, истинность события и власть над изменением

Криптографический отпечаток (Cryptographic Hash), дерево Меркла (Merkle Tree) или журнал с обнаружением вмешательства (Tamper-Evident Log) подтверждают, что связанная с зафиксированным отпечатком копия не менялась незаметно.

Документация инфраструктуры бесключевой подписи (Keyless Signature Infrastructure, KSI) описывает проверку времени подписи, целостности и порядка данных и отпечатка входа. Источник — поставщик, поэтому описание не считается независимой проверкой всех заявлений продукта. ^[12]

Доказательство целостности не устанавливает истинность исходного события, полномочие оператора при вводе или то, что законное изменение не было ошибочно заблокировано. Нужны три связанные плоскости: корректность ввода через рабочие процедуры и доказательства; целостность копии через криптографию и журналы; полномочие на изменение через идентичность, подпись и правовую проверку.

Цепочка происхождения полезна, когда помогает выбрать заведомо целую копию, установить автора изменения и его полномочие и определить откат. Ее роль возрастает при отравлении данных (Data Poisoning), присвоении личности и автоматизации, быстро распространяющей ошибку по всем копиям.

Модель полномочий в чрезвычайной ситуации

Техническая способность восстановить систему не должна совпадать с правом отдать такую команду. Предлагаются четыре отдельные функции: носитель законного полномочия принимает решение; хранители долей ключа исполняют его при достижении порога; оператор запускает резервную среду; независимый аудитор проверяет запрос, журнал и результат.

Нужны заранее определенные чрезвычайные состояния, преемственность, каналы возражения, политика конфликтующих приказов и журнал решений, который одна сторона не может стереть. Нужно подтверждать личность инициатора при отказе основного поставщика идентификации и испытывать отсутствие должностного лица или разрыв связи между органами.

Иностранный хост или коммерческий поставщик не должен разрешать конституционный спор. Соглашение, договор и технический протокол должны одинаково ясно определять разрешенные и запрещенные действия хоста, сохранение активов при неопределенном представительстве и передачу другому хосту.

Предлагаемая матрица рисков

Матрица располагает риски по вероятности причины и влиянию на суверенную функцию. Категории включают физический, кибернетический, операционный, правовой, политический риск, риск поставщика и внутренней власти. Для каждого фиксируются затронутый актив, общая точка отказа, профилактика, обнаружение, путь восстановления и доказательство для закрытия испытания.

Сценарии включают потерю двух площадок; разрыв международного канала; внезапный юридический запрет в принимающей стране; отказ общей панели управления; кражу доли ключа; правомерное, но ошибочное удаление, размноженное синхронизацией; конфликт запросов; невозможность сменить алгоритм. Низкая вероятность некоторых событий сочетается с достаточно высоким ущербом, чтобы оправдать учение или контрмеру.

Матрица должна показывать остаточный риск, а не перекрашивать все ячейки в зеленый. Она различает потерю конфиденциальности, доступности, достоверности доказательства и применение действительного полномочия с неправомерной целью. Снижение одного риска может увеличить другой: высокий порог лучше защищает от захвата, но замедляет восстановление.

Проверяемые аналитические гипотезы

Первая гипотеза: географическое распределение сокращает простой только тогда, когда охватывает рабочие зависимости — идентичность, ключи, управление и связь. Проверка сравнивает распределенное по площадкам, но централизованно управляемое восстановление с вариантом, где есть альтернативные управление и идентификация, при максимально одинаковых функции и данных.

Вторая гипотеза: распределенная власть над ключом снижает риск единоличного захвата, но может увеличить время восстановления и ошибки людей. Изменяются порог, число хранителей и отсутствие некоторых из них; измеряются время разрешения, ошибки и отклоненные запросы. Преимущество схемы «три из пяти» не предполагается заранее, а определяется моделированием риска и учением.

Третья гипотеза: копия с проверяемым происхождением сокращает поиск целой версии после вмешательства, если отпечатки доверия и журналы полномочий независимы от пораженной системы. Четвертая: заранее определенный управляемый ограниченный режим (Controlled Degraded Mode) быстрее возвращает полезный публичный результат, чем полное восстановление, не нарушая права, если каждое применение проверяется.

Гипотезы не содержат скрытых результатов. Испытание может показать, что сложность съела выгоду, конкретная функция не допускает внешнего размещения или независимый внутренний путь дешевле и устойчивее. Ценность прототипа — получить эти ответы до возникновения долгой зависимости.

Рамка экономической оценки

Следует сравнивать стоимость жизненного цикла и стоимость перерыва, а не счет за хранилище и отсутствие расходов. Жизненный цикл включает создание, подключение, испытания, обучение, аудит, договоры, ротацию ключей, смену алгоритмов и выход. Перерыв включает утраченные транзакции, ручную работу, задержку прав, восстановление доверия и последствия для других организаций.

Исходную линию можно построить на обезличенных внутренних инцидентах и тестах, затем измерить время возврата, потерю данных, трудозатраты и цену перехода на резервный режим. Движение рынка или одна война не должны превращаться в постоянный финансовый коэффициент: эффект зависит от функции, длительности, альтернатив и ожиданий сторон.

Нужно оценить зависимость от поставщика и принимающего государства. Сколько стоит переход при изменении права или договора? Сколько времени нужно для извлечения данных, ключей и журналов в применимом формате? Регулярный тест выхода точнее неиспытанной договорной оговорки и показывает, существует ли заявленное разнообразие в работе или только на бумаге.

Проверяемые критерии оценки

Первый критерий функциональный: для каждой критической услуги задается минимальный результат, которым может воспользоваться гражданин или орган, а не просто работающий сервер. Временные метрики — целевое время восстановления (Recovery Time Objective, RTO), предельный простой до неприемлемого воздействия, и целевая точка восстановления (Recovery Point Objective, RPO), момент отката и допустимая потеря относительно последней копии. [13]

Второй критерий — независимость: тест успешен при потере заданного числа площадок или хранителей и при отказе общего поставщика, идентичности либо связи. Независимость измеряется найденными общими зависимостями, а не городами на карте. Третий — целостность восстановления: отравленная или неразрешенная копия выявляется до запуска, а происхождение выбранной копии доказывается.

Четвертый критерий — правильность полномочия: запрос без порога или от неуполномоченного лица не исполняется, а преемственность работает при отсутствии должностного лица. Пятый — выход: данные, ключи, программы и журналы переносятся к другому хосту в известные срок и стоимость. Шестой — соблюдение норм: до реальных данных подтверждены классификация, цель, основание, минимизация и решения компетентных органов. Это предлагаемые метрики, а не заявление об уже пройденном тесте.

Поэтапный прототип

Первый этап использует синтетические данные (Synthetic Data) и нечувствительную услугу, повторяющую структуру реальной государственной функции. Команда строит цепочку зависимостей, задает RTO и RPO, затем создает зашифрованное хранение, резервную рабочую среду, распределенный ключ и аудит. Не следует брать реальные персональные данные для идеи, которую можно проверить без них.

Второй этап — составные отказы под независимым наблюдением: потеря площадок, отсутствие хранителей, разрыв связи, отравленная копия, неразрешенный запрос, переход к другому поставщику. Фиксируются время,

решения, человеческие ошибки и зависимости, которых не было на схеме. Одно удачное восстановление не доказывает постоянной готовности.

К более чувствительным данным или функциям переходят лишь после независимой правовой, технической и приватностной проверки, устранения существенных дефектов и доказанного выхода. Испытание может исключить внешнее размещение для определенной категории — это корректный результат, если его дала проверка, а не заранее выбранный лозунг.

Реализация и управление

У функции должен быть владелец, а не только владелец хранилища. Ведомство реестра знает последствия утраты; цифровой орган ведет интеграцию; орган кибербезопасности проверяет защиту и реагирование; регулятор — передачу и приватность; внешнеполитическое ведомство — правовой статус. Ответственность за принятие риска должна быть записана, а не рассеяна до исчезновения.

Договоры должны давать права аудита, уведомление об инцидентах, перечень мест обработки и подрядчиков, гарантии возврата активов и уничтожения копий, помощь при переходе. Соблюдение норм нельзя доказывать только отчетом поставщика. Межгосударственное соглашение регулирует вход, арест, связь, право, спор, прекращение и представительство.

Долгоживущим активам нужна криптографическая гибкость (Cryptographic Agility): учет алгоритмов, сертификатов и ключей, их максимальное отделение от приложений, план ротации и повторного шифрования. Утверждение NIST стандартов FIPS 203, 204 и 205 в августе 2024 года не доказывает крах нынешнего шифрования, но показывает, что смена алгоритма — операционное событие, способность к которому проектируют заранее. ^[16]

Ограничения и неопределенность

Часть случаев основана на государственных или журналистских сообщениях без полных операционных журналов. Открытые источники не раскрывают всех деталей восстановления Украины, точного состояния каждого документа Судана

или влияния каждого сбоя на каждую услугу. Факты используются только в доказанных пределах, не как всеобъемлющий аудит.

Сопоставление правовых архивов, семян и государственных систем — ограниченная функциональная аналогия, а не материальное равенство. Модель Шамира дает математическую гарантию в своих предпосылках, но не доказывает безопасность реализации и независимость хранителей. Документы KSI описывают продукт со слов поставщика и не устанавливают истинность исходных данных или применение во всех услугах Эстонии.

Работа не содержит саудовских данных о стоимости, измерений производительности или оценки соответствия. Геополитические и правовые риски меняются. Исполнительное решение требует актуальных моделей угроз, классификации, испытаний, договоров, соглашений и независимых проверок.

Отбор случаев подвержен смещению доступности: задокументированные государством, судом или медиа события легче изучать, чем внутренне устраненные или секретные сбои. Объявленный успех может скрывать остановку вторичных услуг, а известный провал — отражать большую прозрачность, а не худшую работу. Число случаев не используется для рейтинга стран или частоты отказов; оно помогает вывести вопросы для конкретной саудовской среды.

Заключение

Посольство данных — возможный инструмент более широкой архитектуры, а не сама архитектура. Соглашение создает правовую защиту, которой не дает торговое имя; распределение повышает устойчивость к отдельным сбоям, если площадки, управление и ключи действительно независимы. Но данные не становятся публичной функцией без программ, идентичности, связи, подписи и полномочий.

Защитимая саудовская модель избирательна и испытана: начинается с функции, определяет допустимые простой и потерю, отделяет власть от владения, включает происхождение и законность разрешения в восстановление и подчиняет передачу нормам и компетентным органам. Для одних функций она может выбрать внутреннюю площадку, для других — защищенное внешнее размещение, для третьих — распределение ключей или доказательств.

Стратегическая ценность не в числе посольств и объеме хранилища, а в доказуемом ответе: после потери площадок, связи и хранителей способно ли государство подтвердить правильное право и исполнить минимальную услугу по законному решению и в срок, который выдерживает общество?

01 · Четыре условия непрерывности

Контрольные рубежи суверенной непрерывности (Sovereign Continuity Gates)

1	2	3	4
Целевое время восстановления (Recovery Time Objective, RTO) и целевая точка восстановления (Recovery Point Objective, RPO)	Правовая и техническая независимость от общей причины (Common-Mode Failure)	Распределенное разрешение при законном пороге (Threshold Authorization)	Испытанное восстановление с проверяемой цепочкой происхождения (Provenance)

Модель не переходит к реальным данным, пока не пройдены все четыре рубежа: определение функции, снижение общих зависимостей, правильность полномочий и доказанное восстановление в пределах допустимых времени и потери.

Источники

1. [Agreement between Estonia and Luxembourg on the hosting of data and information systems](#)
Riigi Teataja, 20 июня 2017 г.
2. [The Legal Status of Data Embassies](#)
International and Comparative Law Quarterly, 1 января 2019 г.
3. [Ukraine's cybersecurity infrastructure protected state registers during the war](#)
President of Ukraine, 6 сентября 2022 г.
4. [Farooq Ahmad Dar v. State of Jammu and Kashmir](#)
High Court of Jammu and Kashmir and Ladakh, 13 апреля 2022 г.
5. [Q&A: Syria's New Property Law](#)
Human Rights Watch, 29 мая 2018 г.

6. 30 million Sudanese historical documents at risk of deterioration
Asharq Al-Awsat, 26 июня 2026 г.
7. Sudan telecommunications joint statement
Norwegian Refugee Council, 3 мая 2024 г.
8. ICARDA seeds safe back in Lebanon and Morocco
Svalbard Global Seed Vault, 27 октября 2017 г.
9. Norges tilstedeværelse i Storbritannia under 2. verdenskrig
National Archives of Norway
10. Engineering Trustworthy Secure Systems
NIST, 1 марта 2022 г.
11. How to Share a Secret
Communications of the ACM, 1 ноября 1979 г.
12. KSI Technology
Guardtime
13. Contingency Planning Guide for Federal Information Systems
NIST, 1 мая 2010 г.
14. Implementing Regulations for Personal Data Transfer outside the Kingdom
SDAIA
15. Cloud Cybersecurity Controls CCC-2:2024
National Cybersecurity Authority
16. NIST Releases First 3 Finalized Post-Quantum Encryption Standards
NIST, 13 августа 2024 г.