

Об утверждении требований по управлению цифровыми данными

Постановление Правительства Республики Казахстан от 22 сентября 2026 года № 830

В соответствии с пунктом 3 статьи 16 Цифрового кодекса Республики Казахстан Правительство Республики Казахстан ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемые требования по управлению цифровыми данными.
2. Признать утратившими силу:
 - 1) постановление Правительства Республики Казахстан от 7 ноября 2024 года № 925 "Об утверждении требований по управлению данными";
 - 2) пункт 75 изменений и дополнений, которые вносятся в некоторые решения Правительства Республики Казахстан и распоряжения Премьер-Министра Республики Казахстан, утвержденных постановлением Правительства Республики Казахстан от 14 июля 2026 года № 615 "О внесении изменений и дополнений в некоторые решения Правительства Республики Казахстан и распоряжения Премьер-Министра Республики Казахстан".
3. Настоящее постановление вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

*Премьер-Министр
Республики Казахстан*

О. Бектенов

Утверждены
постановлением Правительства
Республики Казахстан
от " " 2026 года №

Требования по управлению цифровыми данными

Глава 1. Общие положения

1. Требования по управлению цифровыми данными (далее – требования) разработаны в соответствии с пунктом 3 статьи 16 Цифрового кодекса Республики Казахстан и определяют требования по управлению цифровыми данными.

2. Положения требований распространяются на государственные органы, государственные юридические лица, субъекты квазигосударственного сектора, (далее – организации), за исключением специальных государственных органов.

При формировании продуктов цифровых данных, размещаемых на платформе обмена и оборота продуктов цифровых данных с соблюдением правил функционирования платформ обмена и оборота продуктов цифровых данных, согласно

пункту 2 статьи 31 Цифрового кодекса Республики Казахстан, государственные органы, государственные юридические лица и субъекты квазигосударственного сектора учитывают требования в отношении структуры, качества и метаданных.

3. Настоящие требования направлены на обеспечение:

возможности однократного предоставления и многократного использования цифровых данных при осуществлении государственных функций и оказании вытекающих из них услуг;

единства цифровой инфраструктуры и способов взаимодействия организаций при осуществлении деятельности по управлению цифровыми данными;

персональной ответственности за качество предоставленных цифровых данных;

недискриминационного доступа физических и юридических лиц к цифровым данным, относящимся к общедоступной информации;

упорядочивания цифровых данных по сходству или различию присущих им характеристик, унификации структурных элементов цифровых данных и форматов их представления;

систематизации описания цифровых данных и связей между ними;

учета прав на получение (предоставление) цифровых данных в процессе интеграции цифровых объектов;

приведения цифровых данных в соответствие с цифровыми данными аналогичного вида путем гармонизации;

преимущественного использования электронных способов управления цифровыми данными;

соблюдения предусмотренных законодательством Республики Казахстан прав обладателей, ограничений на доступ к данным, отнесенным к конфиденциальной информации и иной охраняемой законом тайне, по обеспечению защиты данных;

соответствия порядка использования цифровых данных этическим нормам;

контроля качества цифровых данных;

онтологического единства цифровых данных, содержащихся в цифровых объектах "цифрового правительства";

баланса между своевременным внедрением цифровых технологий обработки цифровых данных и защитой прав на неприкосновенность частной жизни, личной и семейной тайны;

централизации управления цифровыми данными с учетом коллегиальности принятия решений и согласованности действий по управлению цифровыми данными;

гибкости подходов к управлению жизненным циклом цифровых данных;

ориентации на пользователя цифровых данных;

определения качества административных цифровых данных.

4. Для целей применения настоящих требований используются следующие определения:

1) аналитический дашборд – информационная панель визуализации результатов аналитики цифровых данных, формируемая инструментами цифровой аналитической системы "Smart Data Ukimet", на основе ее единого хранилища данных;

2) реестр аналитических дашбордов – централизованный перечень, в котором собрана и структурирована информация обо всех существующих дашбордах в государственных органах и организациях;

3) архитектурно-координационный центр (далее - центр) – юридическое лицо, определяемое Правительством Республики Казахстан;

4) атрибут – характеристика сущности, позволяющая ее идентифицировать, описать или измерить (на физическом уровне атрибуту сущности могут соответствовать столбец, поле, тег или узел (место пересечения) в таблице, представлении, документе, графе или файле);

5) административные данные – индивидуальные количественные (измеряемые с помощью чисел) и (или) качественные (выстроенные по определенному принципу и (или) признаку) данные по физическому или юридическому лицу и данные хозяйственного учета, собираемые и (или) обрабатываемые, и (или) формируемые административными источниками, за исключением первичных статистических и альтернативных данных (административными данными могут быть административные цифровые данные);

6) административные цифровые данные – цифровые данные, формируемые государственными органами, государственными юридическими лицами, субъектами квазигосударственного сектора и субъектами при исполнении возложенных на них государственных функций и оказании государственных услуг;

7) определение качества административных цифровых данных – процесс анализа результатов оценки качества цифровых данных, в том числе административных цифровых данных, устанавливающий степень пригодности цифровых данных к использованию в соответствии с законодательством Республики Казахстан;

8) данные – информация в формализованном виде, пригодная для обработки;

9) библиотека данных – совокупность структурированных и (или) сгруппированных данных, пригодных для обучения моделей искусственного интеллекта;

10) формирование контрольной суммы библиотеки данных – процесс создания уникального цифрового кода с помощью хеш-функции или специального алгоритма на основе содержимого библиотеки данных, используемый для проверки ее целостности и обнаружения искажений;

11) база данных (далее – БД) – совокупность систематизированных данных, пригодных для обработки посредством цифровых технологий;

12) способы интеграции данных: "извлекать", "преобразовывать", "загружать" (Extract, Transform, Load) (далее – ETL) – процесс, основанный на извлечении, преобразовании и загрузке данных из источника в хранилище данных;

13) способ интеграции данных: "сбор данных об изменениях" (Change Data Capture) (далее – CDC) – процесс, основанный на идентификации, регистрации и доставке изменений, внесенных в БД;

14) концептуальная модель данных домена – модель данных домена, представленная в виде основных сущностей домена с ключевыми атрибутами и связей между ними;

15) оператор национальной платформы искусственного интеллекта (далее – оператор НП ИИ) – юридическое лицо, на которое возложено обеспечение развития и функционирования национальной платформы искусственного интеллекта;

16) архитектурный портал цифровых объектов государства – цифровой объект, предназначенный для осуществления учета, хранения и систематизации сведений о цифровых объектах государства, цифровой архитектуре государства, платформенных программных продуктах, дальнейшего использования государственными органами для мониторинга, анализа и планирования в сфере цифровизации;

17) национальный регистр – цифровой ресурс, содержащий эталонные цифровые данные, определенные в рамках архитектуры "цифрового правительства" и используемые в качестве единого источника достоверной информации для выполнения государственных функций, оказания государственных услуг, межведомственного взаимодействия и государственной статистики;

18) неоцифрованные данные – данные в бумажном виде, не содержащиеся в цифровых объектах;

19) цифровые данные – информация, предоставленная в цифровой форме и пригодная для автоматизированного и (или) аналитического сбора, хранения, обработки, использования, передачи, распространения или удаления независимо от способа ее получения и формы цифрового предоставления;

20) аналитика цифровых данных – процесс обработки цифровых данных с целью получения информации и выводов для принятия решения;

21) заказчик аналитики цифровых данных – государственные органы и организации ;

22) качество цифровых данных – характеристика, показывающая степень пригодности данных к использованию в соответствии с законодательством Республики Казахстан;

23) оценка качества цифровых данных – измерение соответствия цифровых данных критериям качества цифровых данных, в том числе установление соответствия административных цифровых данных национальным регистрам;

24) критерии качества цифровых данных – общепринятые критерии качества цифровых данных, используемые для оценки и контроля критических критериев

качества цифровых данных, таких как точность, полнота, взаимосвязанность, сопоставимость, актуальность, уникальность, достоверность, своевременность, ясность, доступность;

25) управление цифровыми данными – процесс, связанный с определением, созданием, сбором, накоплением, хранением, распространением, уничтожением, поддержкой цифровых данных, а также обеспечением их аналитики, качества, доступности, защиты;

26) уполномоченный орган по управлению цифровыми данными (далее – уполномоченный орган) – центральный исполнительный орган, осуществляющий руководство и межотраслевую координацию по управлению цифровыми данными;

27) сбор цифровых данных – действия, направленные на получение цифровых данных;

28) обезличивание цифровых данных – действия, в результате совершения которых идентификация объекта описания невозможна;

29) обработка цифровых данных – действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование, архивирование и уничтожение данных;

30) пользователь цифровых данных – физическое или юридическое лицо, запрашивающее и (или) использующее цифровые данные;

31) хранение цифровых данных – действия по обеспечению целостности, конфиденциальности и доступности цифровых данных;

32) оператор "цифрового правительства" (далее – оператор) – юридическое лицо, определяемое Правительством Республики Казахстан, которое обеспечивает функционирование цифровых объектов "цифрового правительства";

33) эталонные цифровые данные – структурированные цифровые данные первичного учета объектов предметной области, которые служат основой для принятия решений;

34) цифровая аналитическая система "Smart Data Ukimet" (далее – SDU) – цифровой объект, предназначенный для формирования единого хранилища данных государственных органов, государственных юридических лиц, субъектов квазигосударственного сектора, как в неструктурированном, так и структурированном виде, для целей предоставления аналитической информации по деятельности Правительства Республики Казахстан.

Данные, создаваемые, накапливаемые и приобретаемые за счет бюджетных средств, а также полученные государственными органами способами, установленными статьей 19 Закона Республики Казахстан "О государственном имуществе", являются государственными.

5. Данные фиксируются на электронном и бумажном носителях. Организации в рамках управления цифровыми данными обеспечивают перевод данных, необходимых

для осуществления государственных функций и оказания государственных услуг, их аналитики, в электронную форму.

6. Управление цифровыми данными подразделяется на следующие виды:
по содержанию:

1) метаданные – данные, описывающие структуру и характеристики данных.

Метаданные подразделяются на следующие виды:

функциональные метаданные: описывают содержание и состояние данных, имеющих прямое отношение к специфике деятельности организации, включая сведения, используемые при обеспечении качества данных;

технические метаданные: описывают технические характеристики данных и систем их хранения;

операционные метаданные: описывают процессы обработки цифровыми данными и управления доступом к ним (сведения, используемые при обеспечении безопасности данных);

2) справочные данные – элементы национальной справочной информации;

3) транзакционные данные – сведения, отражающие результат изменения данных, относящиеся к фиксированному моменту времени, не изменяющиеся в будущем;

по характеру организации данных:

1) неструктурированные данные – данные в неформализованном виде, сложном или не пригодном для обработки;

2) структурированные данные – упорядоченные данные, пригодные для обработки.

7. Жизненный цикл цифровых данных состоит из следующих этапов:

создание (сбор) цифровых данных;

хранение цифровых данных и их ведение;

использование цифровых данных;

управление цифровыми данными;

архивирование цифровых данных (или их уничтожение).

8. В целях управления цифровыми данными организации обеспечивают определение:

1) лица, ответственного за управление цифровыми данными в курируемой отрасли, стратегические направления и определение политики управления цифровыми данными;

2) лица, ответственного за управление цифровыми данными (менеджер по данным), в функции которого входят:

мониторинг соблюдения настоящих требований и политики управления цифровыми данными;

координация за своевременным наполнением БД актуальными, полными и аутентичными сведениями соответствующими ответственными лицами;

проведение внутреннего контроля на предмет аутентичности цифровых данных в SDU с аналогичными цифровыми данными, размещенными в цифровых объектах "цифрового правительства";

мониторинг за своевременным внесением посредством интеграции сведений по показателям (отраслевым данным) в SDU и проведение верификации показателей;

обеспечение размещения интеграционных сервисов в реестре сервисов;

координация работы по заполнению паспортов данных цифровых объектов (далее – паспорт данных), описанию видов цифровых данных, их данных;

разработка и согласование внутренних актов по управлению цифровыми данными;

проверка проектной и технической документации на создание и развитие цифровых объектов на соответствие настоящим требованиям;

проведение мероприятий по обучению и повышению уровня квалификации сотрудников в части управления цифровыми данными;

обеспечение бесперебойного функционирования принадлежащих организации БД;

обеспечение внедрения технологий управления цифровыми данными;

организация соблюдения требований защиты данных в рамках всего жизненного цикла цифровых данных.

Глава 2. Требования к определению, созданию, сбору, обработке и накоплению цифровых данных

Параграф 1. Требования к определению цифровых данных

9. В целях определения цифровых данных, содержащихся в БД организаций, формируется и ведется каталог цифровых данных (далее – каталог), являющийся систематизированным перечнем сведений о видах цифровых данных и связях между ними.

Каталог подлежит актуализации при каждом изменении структуры и (или) источников цифровых данных.

10. Уполномоченный орган осуществляет согласование сформированного организациями перечня сведений об основных (мастер) данных в каталоге.

11. Целями формирования и ведения каталога являются:

формирование единого источника информации о составе и структуре цифровых данных организации;

создание условий для совместного использования цифровых данных организациями в рамках цифровой трансформации государственного управления;

структурирование цифровых данных;

обеспечение качества цифровых данных;

создание правовых условий для обеспечения доступа к цифровым данным организации;

проведение аналитики цифровых данных;

поиск и проверка учтенных в каталоге сведений о цифровых данных, включая сведения об эталонных цифровых данных, путем интеграции цифровых объектов;

формирование перечня открытых цифровых данных государственных органов, размещаемых на интернет-портале открытых цифровых данных;

формирование цифровых профилей по объектам описания;

приведение цифровых данных в соответствие с цифровыми данными аналогичного вида согласно требованиям, установленным законодательством Республики Казахстан, путем гармонизации.

12. Каталог формируется на архитектурном портале цифровых объектов государства центром и организациями путем формирования паспортов цифровых данных цифровых объектов по форме, согласно приложению 1 к настоящим требованиям. При изменении структуры цифровых данных, источников данных, формул расчета показателей и описания неоцифрованных данных паспорт объекта подлежит актуализации.

Паспорт цифровых данных и описание неоцифрованных данных согласовываются менеджером по цифровым данным и центром.

По создаваемым и (или) развиваемым цифровым объектам формирование паспорта цифровых данных, описание неоцифрованных данных и их согласование осуществляются организациями до введения в промышленную эксплуатацию цифрового объекта.

13. Каталог ведется на архитектурном портале цифровых объектов государства центром.

Под ведением каталога понимается обеспечение организационных и технических условий для его ведения.

14. Центром в рамках формирования цифровой архитектуры правительства обеспечиваются:

техническая возможность формирования и ведения паспортов цифровых данных и описания неоцифрованных данных на архитектурном портале цифровых объектов государства;

защита сведений, содержащихся в каталоге, в соответствии с едиными требованиями в сферах цифровизации и обеспечения кибербезопасности, утвержденными постановлением Правительства Республики Казахстан (далее – ЕТ);

техническая, методическая и информационная поддержка по вопросам формирования паспортов цифровых данных и описания неоцифрованных данных на архитектурном портале цифровых объектов государства;

формирование цифровых профилей по объектам описания.

Центр уведомляет оператора о сформированных паспортах цифровых данных и описании неоцифрованных данных с возможностью доступа к чтению каталога.

15. Организации (отраслевые эксперты) совместно с центром формируют источники эталонных цифровых данных с описанием детальной передачи цифровых данных цифровым объектам, БД, проведением анализа бизнес-процессов.

16. В цифровых объектах не допускается определение эталонных цифровых данных, предусмотренных другим цифровым объектом.

17. Перечень национальных регистров, их структура, состав эталонных цифровых данных, а также требования к их ведению и актуализации определяются уполномоченным органом в сфере цифровизации по согласованию с уполномоченным органом в области государственной статистики согласно пункту 2 статьи 19 Цифрового кодекса Республики Казахстан.

Собственники и (или) владельцы цифровых объектов, являющиеся держателями или источниками цифровых данных для национальных регистров, обеспечивают надлежащее качество цифровых данных, содержащихся в национальных регистрах, в соответствии с законодательством Республики Казахстан.

18. Эталонные цифровые данные используются для сверки с ними аналогичного вида цифровых данных в целях выявления и фиксирования наличия противоречий между эталонными цифровыми данными и данными, содержащимися в цифровых объектах, и последующего устранения противоречий.

19. Доступ к сведениям, содержащимся в каталоге, предоставляется организациям на безвозмездной основе.

Доступ к сведениям о видах цифровых данных, сформированных в каталоге на основе сведений, являющихся общедоступной информацией, размещаемой в форме открытых данных, предоставляется физическим и юридическим лицам на безвозмездной основе.

Доступ к сведениям каталога, содержащим персональные данные и иную охраняемую законом информацию, осуществляется с учетом требований и особенностей, установленных законодательством Республики Казахстан в сфере персональных данных и их защиты.

20. Описание неоцифрованных данных осуществляется по форме согласно приложению 2 к настоящим требованиям.

Данные организаций в бумажном виде, электронных таблицах, реестрах включаются и заполняются в описание неоцифрованных данных.

Описание неоцифрованных данных осуществляется по трем этапам:

1) формирование неоцифрованных данных на основе анализа текущих данных организаций и проведения анализа законодательства Республики Казахстан;

2) формирование эталонных цифровых данных по субъектам и объектам данных из анализа законодательства Республики Казахстан, выявление сущности, определение для каждой сущности уникального набора атрибутов;

3) формирование взаимосвязи между сущностями для создания концептуальной модели данных домена, представленной в виде основных сущностей домена с ключевыми атрибутами и связей между ними.

Параграф 2. Требования к созданию, сбору, обработке и накоплению цифровых данных

21. Создание, сбор, обработка и накопление цифровых данных организациями осуществляются в объеме, необходимом и достаточном для выполнения возложенных на них функций и задач.

22. При управлении цифровыми данными организации обеспечивают применение и повторное использование цифровых данных (с учетом необходимых изменений), новые способы создания и использования цифровых данных в зависимости от нужд конечных потребителей на основе аналитики цифровых данных, при этом не допускается повторный сбор цифровых данных при их наличии в цифровых объектах "цифрового правительства".

При отсутствии собираемых или истребуемых цифровых данных от физических и юридических лиц в цифровых объектах "цифрового правительства" такие сбор и истребование осуществляются путем автоматизации.

23. Создание, сбор, обработка и накопление цифровых данных осуществляются в соответствии с архитектурой цифровых данных, являющейся слоем цифровой архитектуры правительства, представляющей собой описание цифрового объекта "цифрового правительства", содержащихся в них цифровых данных, интеграции, подходов и средств управления цифровыми данными.

24. При создании, сборе, обработке и накоплении цифровых данных государственные органы осуществляют ведение элементов национальной справочной информации в цифровом объекте уполномоченного органа в области государственной статистики.

25. При сборе цифровых данных от физических и юридических лиц организациями обеспечиваются идентификация круга лиц, представляющих информацию, и применение элементов национальной справочной информации.

26. Архитектура цифровых данных формируется центром на основе каталога, включая паспорта цифровых данных и описания неоцифрованных данных.

27. Проектирование концептуальной модели цифровых данных домена осуществляется при формировании архитектуры цифровых данных доменов центром совместно с организациями на основании паспортов цифровых данных.

Организации ежемесячно, 5 числа каждого месяца, следующего за отчетным, осуществляют проверку актуальности сведений в концептуальной модели цифровых данных домена и вносят соответствующие изменения в каталог.

Внесение изменений в каталог согласовывается менеджером по цифровым данным и центром.

Внесение изменений в архитектуру цифровых данных осуществляется центром в соответствии со статьей 69 Цифрового кодекса Республики Казахстан.

28. В соответствии с цифровой архитектурой правительства организации передают (мигрируют) цифровые данные на платформу "цифрового правительства".

Организации предоставляют доступ оператору "цифрового правительства" к цифровым данным и цифровым записям для осуществления аналитики данных.

Глава 3. Требования к качеству и поддержке цифровых данных

Параграф 1. Организация управления качеством цифровых данных

29. Управление качеством цифровых данных предполагает организацию согласованной деятельности по контролю следующих критериев качества цифровых данных:

точность (критерий качества цифровых данных, определяющий необходимый уровень детализации цифровых данных);

полнота (критерий качества цифровых данных, определяющий достаточность заполнения наборов цифровых данных и их атрибутов);

взаимосвязанность (критерий качества цифровых данных, определяющий насколько непротиворечивыми являются цифровые данные в различных связанных наборах цифровых данных);

сопоставимость (критерий качества цифровых данных, определяющий насколько данные из разных источников или за разные периоды времени могут быть сопоставимы и использованы);

актуальность (критерий качества цифровых данных, определяющий степень соответствия цифровых данных моделируемой области на определенный момент времени);

уникальность (критерий качества цифровых данных, определяющий отсутствие дублирования цифровых данных);

достоверность (критерий качества цифровых данных, определяющий насколько корректно цифровые данные описывают моделируемую область);

своевременность (критерий качества цифровых данных, определяющий доступность цифровых данных пользователю в нужный момент времени);

ясность (критерий качества цифровых данных, определяющий легкость интерпретации и использования пользователем);

доступность (критерий качества цифровых данных, определяющий наличие равного доступа к цифровым данным).

Определение качества цифровых данных по критериям ясности и доступности осуществляется исключительно в отношении органов государственной статистики.

Уполномоченный орган в области определения качества административных цифровых данных при определении качества административных цифровых данных запрашивает их метаданные, паспорта и каталоги данных при их отсутствии на архитектурном портале цифровых объектов государства у организации с соблюдением требований, предусмотренных законодательством Республики Казахстан о государственных секретах и иной охраняемой законом Республики Казахстан тайне.

Несоответствие цифровых данных одному из критериев качества цифровых данных является основанием для определения их недостоверными.

30. Оператор на ежеквартальной основе совместно с собственником и (или) владельцем цифровых объектов "цифрового правительства" осуществляет верификацию цифровых данных на предмет аутентичности цифровых данных и цифровых записей в SDU с аналогичными цифровыми данными, размещенными в цифровых объектах "цифрового правительства".

31. Проведение мероприятий по обеспечению и повышению качества цифровых данных осуществляется в три этапа:

1) планирование мероприятий по обеспечению и повышению качества цифровых данных;

2) проведение мероприятий по обеспечению и повышению качества цифровых данных;

3) оценка эффективности проведения мероприятий по обеспечению и повышению качества цифровых данных.

32. Мероприятия по повышению качества цифровых данных по критерию качества "Точность":

в целях обеспечения и повышения качества цифровых данных в части выполнения требований к достоверности цифровых данных организация проводит мероприятия по устранению (или сокращению влияния) причин, влияющих на не соответствующие требованиям значения индикаторов качества цифровых данных, относящихся к критерию "Точность", направленные на:

разработку и внедрение стандартных операционных процедур для сбора, ввода и обработки цифровых данных, в том числе использование унифицированных методов и инструментов;

внедрение процедур проверки и валидации цифровых данных на всех этапах их жизненного цикла;

осуществление проверки цифровых данных на предмет выявления аномальных значений.

33. Мероприятия по повышению качества цифровых данных по показателю "Полнота":

в целях обеспечения и повышения качества цифровых данных в части выполнения требований к достоверности цифровых данных организация организует и проводит

мероприятия по устранению (или сокращению влияния) причин, влияющих на не соответствующие требованиям значения индикаторов качества цифровых данных, относящихся к критерию "Полнота", направленные на:

- уточнение атрибутов цифровых данных, обязательных к заполнению, и соответствующего порядка контроля качества цифровых данных;

- периодическую проверку и выявление незаполненных атрибутов цифровых данных, устранение выявленных ошибок и несоответствий цифровых данных непосредственно в цифровых объектах "цифрового правительства";

- совершенствование (усиление) форматно-логического контроля при обработке цифровых данных в цифровых объектах "цифрового правительства" в части контроля заполненности атрибутов цифровых данных, развитие (доработка) форм ввода цифровых данных цифровых объектов "цифрового правительства", осуществляющего сбор и обработку цифровых данных;

- установление источников цифровых данных, позволяющих дополнить (обогащить) цифровые данные, и проведение гармонизации (обогащения) цифровых данных с установленными источниками цифровых данных;

- оптимизацию процессов обработки цифровых данных (сокращение ручного ввода цифровых данных).

34. Мероприятия по повышению качества цифровых данных по критерию качества "Взаимосвязанность":

в целях обеспечения и повышения качества цифровых данных в части выполнения требований к достоверности цифровых данных организация организует и проводит мероприятия по устранению (или сокращению влияния) причин, влияющих на не соответствующие требованиям значения индикаторов качества цифровых данных, относящихся к критерию "Взаимосвязанность", направленные на:

- взаимную непротиворечивость цифровых данных;

- установление источников эталонных цифровых данных;

- гармонизацию цифровых данных с установленными источниками цифровых данных;

- гармонизацию цифровых данных с актуальными элементами национальной справочной информации.

35. Мероприятия по повышению качества цифровых данных по критерию качества "Сопоставимость":

в целях обеспечения и повышения качества цифровых данных в части выполнения требований к достоверности цифровых данных организация организует и проводит мероприятия по устранению (или сокращению влияния) причин, влияющих на не соответствующие требованиям значения индикаторов качества цифровых данных, относящихся к критерию "Сопоставимость", направленные на:

- использование эталонных цифровых данных;

сравнение цифровых данных во временном, региональном и отраслевом разрезах;
интеграцию цифровых объектов;
использование актуальных элементов национальной справочной информации.

36. Мероприятия по повышению качества цифровых данных по критерию "Актуальность":

в целях обеспечения и повышения качества цифровых данных в части выполнения требований к достоверности цифровых данных организация организует и проводит мероприятия по устранению (или сокращению влияния) причин, влияющих на не соответствующие требованиям значения индикаторов качества цифровых данных, относящихся к критерию "Актуальность", направленные на:

установление порядка выявления цифровых данных, требующих актуализации (например, определение срока устаревания цифровых данных), и определение порядка и периодичности проведения актуализации цифровых данных;

определение степени соответствия цифровых данных текущим и возможным потребностям использования в производстве официальной статистической информации ;

получение актуальных цифровых данных из цифровых объектов на регулярной основе.

Организации, ответственные за наполнение цифровых данных в цифровых объектах , обеспечивают на постоянной основе актуальность цифровых данных, используемых для осуществления государственных функций и оказания государственных услуг.

37. Мероприятия по повышению качества цифровых данных по критерию качества "Уникальность":

в целях обеспечения и повышения качества цифровых данных в части выполнения требований к достоверности цифровых данных организация организует и проводит мероприятия по устранению (или сокращению влияния) причин, влияющих на не соответствующие требованиям значения индикаторов качества цифровых данных, относящихся к критерию "Уникальность", направленные на:

уточнение атрибутов (группы атрибутов) цифровых данных, дублирование значений которых не допускается (уникальность), и порядка выявления повторяющихся записей (сопоставления записей), периодичность выявления повторяющихся записей и их устранения (объединения или удаление цифровых данных);

совершенствование (усиление) форматно-логического контроля при обработке цифровых данных в части внедрения порядка выявления повторяющихся записей (дублей).

38. Мероприятия по повышению качества цифровых данных по критерию "Достоверность":

в целях обеспечения и повышения качества цифровых данных в части выполнения требований к достоверности цифровых данных организация организует и проводит мероприятия по устранению (или сокращению влияния) причин, влияющих на не соответствующие требованиям значения индикаторов качества цифровых данных, относящихся к критерию "Достоверность", направленные на:

- уточнение порядка контроля значений атрибутов цифровых данных (например, выявление аномальных значений, контроля интервальных значений, соответствие маскам ввода, выявление противоречий), совершенствование (усиление) форматно-логического контроля при обработке цифровых данных в цифровых объектах "цифрового правительства";

- установление источников цифровых данных, позволяющих сверить цифровые данные, определить эталонные источники цифровых данных;

- формирование порядка и периодичности гармонизации цифровых данных с эталонными источниками цифровых данных, национальной справочной информации;

- формирование порядка и периодичности сопоставления цифровых данных с установленными источниками цифровых данных в целях выявления расхождений в цифровых данных и устранения выявленных расхождений.

39. Мероприятия по повышению качества цифровых данных по критерию качества "Своевременность":

в целях обеспечения и повышения качества цифровых данных в части выполнения требований к достоверности цифровых данных организация организует и проводит мероприятия по устранению (или сокращению влияния) причин, влияющих на не соответствующие требованиям значения индикаторов качества цифровых данных, относящихся к критерию "Своевременность", направленные на:

- взаимную непротиворечивость цифровых данных;

- установление источников эталонных цифровых данных;

- гармонизацию цифровых данных с установленными источниками цифровых данных;

- получение административных цифровых данных в сроки, соответствующие установленным целям;

- доступность цифровых данных пользователю в нужный момент времени;

- представление административных цифровых данных для проведения государственного контроля в области государственной статистики.

40. Мероприятия по повышению качества цифровых данных по критерию качества "Ясность":

в целях обеспечения и повышения качества цифровых данных в части выполнения требований к достоверности цифровых данных организация организует и проводит

мероприятия по устранению (или сокращению влияния) причин, влияющих на не соответствующие требованиям значения индикаторов качества цифровых данных, относящихся к критерию "Ясность", направленные на:

- представление цифровых данных в удобно читаемой и структурированной форме (таблицы, графики, диаграммы);

- включение аннотаций и метаданных, которые поясняют значения цифровых данных и контекст их использования;

- применение методов визуализации цифровых данных (диаграммы, интерактивные и информационные панели);

- проведение тестирования цифровых данных на предмет их доступности и понятности для целевой аудитории (фокус группы, опросы).

41. Мероприятия по повышению качества цифровых данных по критерию качества "Доступность":

в целях обеспечения и повышения качества цифровых данных в части выполнения требований к достоверности цифровых данных организация организует и проводит мероприятия по устранению (или сокращению влияния) причин, влияющих на не соответствующие требованиям значения индикаторов качества цифровых данных, относящихся к критерию "Доступность", направленные на:

- простоту получения и легкость передачи цифровых данных;

- обеспечение безопасности и конфиденциальности цифровых данных;

- регулярное обновление и архивирование цифровых данных.

42. Планирование проведения мероприятий по обеспечению и повышению качества цифровых данных осуществляется на основе мониторинга и анализа результатов оценок качества цифровых данных, в том числе определения качества административных цифровых данных.

43. Проведение мероприятий по обеспечению и повышению качества цифровых данных осуществляется на постоянной основе в целях устранения или сокращения влияния причин, влияющих на снижение значений индикаторов качества цифровых данных.

44. В рамках управления качеством цифровых данных организации обеспечивают формирование логов БД в части отслеживания изменения цифровых данных в эталонных БД через CDC.

45. В целях повышения качества цифровых данных центр проводит анализ цифровых данных, формируемых организациями, и дает рекомендации по повышению качества цифровых данных для исполнения организациями.

46. В мониторинге качества цифровых данных задействуется весь персонал организации, участвующий в обработке цифровых данных, в соответствии с принятым организацией порядком проверки и обеспечения качества цифровых данных.

47. Объектом оценки качества цифровых данных являются данные, содержащиеся в цифровом объекте и соответствующие перечню цифровых данных, включенных в каталог.

48. Внутреннюю оценку качества цифровых данных в организации осуществляет менеджер по управлению данными в соответствии с принятым организацией порядком проверки и обеспечения качества цифровых данных, предусматривающим:

- 1) определение текущих значений критериев качества цифровых данных;
- 2) оценку полученных значений критериев качества цифровых данных;
- 3) фиксацию результатов внутренней оценки качества цифровых данных;
- 4) устранение выявленных несоответствий критериям качества цифровых данных.

49. Оценка качества цифровых данных в инициативном порядке осуществляется пользователями цифровых данных.

50. Оценка качества цифровых данных проводится в организации, осуществляется в отношении каждого вида цифровых данных на регулярной основе с учетом установленных порядком проверки и обеспечения качества цифровых данных требований к частоте (периодичности) и способу проведения регулярной оценки.

51. Результаты внутренней оценки качества цифровых данных подлежат анализу центром и определению качества административных цифровых данных уполномоченным органом в области определения качества административных цифровых данных, а также являются исходными цифровыми данными для проведения мероприятий по повышению качества цифровых данных.

Параграф 2. Требования к поддержке цифровых данных

52. В целях поддержки качества цифровых данных организация регламентирует, организует и проводит следующие мероприятия:

- 1) постоянный мониторинг качества цифровых данных, направленный на:
 - отработку инцидентов качества цифровых данных;
 - выявление ошибок и несоответствий цифровых данных;
 - совершенствование (усиление) форматно-логического контроля при обработке цифровых данных;
 - оптимизацию процессов обработки цифровых данных;
 - систематизацию и гармонизацию цифровых данных;
- 2) обучение (повышение квалификации) персонала, участвующего в обработке цифровых данных;
- 3) организацию оценки качества цифровых данных.

53. Под ошибками в цифровых данных понимаются:

техническая ошибка – опечатка, грамматическая или арифметическая ошибка и ошибка, допущенная при сборе и обработке цифровых данных, приведшая к несоответствию сведений, содержащихся в цифровом объекте, сведениям,

содержащимся в документах, на основании которых вносились сведения в цифровой объект;

несоответствие цифровых данных, относящихся к требованиям, установленным законодательством Республики Казахстан, и регламентирующих процессы сбора и обработки цифровых данных.

54. Техническая ошибка выявляется:

организацией и (или) пользователями в процессе сбора и обработки цифровых данных в рамках межведомственного взаимодействия при выполнении государственных функций и оказании государственных услуг;

уполномоченным органом в области определения качества административных цифровых данных при определении качества административных цифровых данных;

оператором при осуществлении аналитики данных.

55. Устранение технических ошибок осуществляется на основании заявления от лиц, указанных в пункте 57 настоящих Правил (далее – заявитель), а также вступившего в законную силу решения суда в установленный срок.

56. При обнаружении технических ошибок в цифровых данных, противоречий или неполноты цифровых данных, относящихся к определенному или определяемому лицу, его имуществу или правам, такое лицо направляет в организацию заявление об исправлении ошибок в цифровых данных или дополнении цифровых данных, которыми управляют организации, в бумажной или электронной форме в течение пяти рабочих дней с момента обнаружения.

При обеспечении сбора и обработки цифровых данных организация самостоятельно исправляет ошибки и неполноту цифровых данных.

При нанесении вреда или нарушении законных интересов заявителя исправление ошибки производится по заявлению в соответствующие уполномоченные органы.

Споры, возникающие в связи с исправлением технических ошибок, не урегулированных в досудебном порядке, рассматриваются в судебном порядке.

Исправление цифровых данных, выявленных при оказании государственных услуг, осуществляется на основании заявления, направленного посредством веб-портала "цифрового правительства", мобильного приложения "цифрового правительства" и интегрированной цифровой системы центров обслуживания населения.

Организация с момента исправления технической ошибки уведомляет заявителя и соответствующих участников отношений, являющихся пользователями цифровых данных, об исправлении технической ошибки в цифровых данных.

57. Ошибки в цифровых данных, связанные с несоответствием цифровых данных требованиям, установленным законодательством Республики Казахстан, подразделяются на виды и фиксируются в инцидентах по соответствующему виду выявленных ошибок:

по покрытию (охвату) – вид инцидента, фиксирующий ошибки, связанные с отсутствием в цифровых данных записей о требуемом (запрашиваемом) объекте описания или группе объектов описания;

по полноте – вид инцидента, фиксирующий ошибки, связанные с неполным заполнением или незаполнением в записях вида цифровых данных атрибутов, относящихся к категории обязательных;

по точности и противоречивости – вид инцидента, фиксирующий ошибки, связанные с несоответствием предоставленных цифровых данных целям использования или цифровым данным, полученным из эталонного источника, и цифровым данным, полученным в результате измерения (инцидент формируется при выявлении противоречий (несоответствия) в цифровых данных, полученных из различных цифровых объектов);

по своевременности – вид инцидента, фиксирующий ошибки, связанные с несоответствием представленных цифровых данных актуальному состоянию на установленные или произвольные моменты времени;

по уникальности – вид инцидента, фиксирующий ошибки, связанные с наличием в представленных уникальных цифровых данных дублей записей;

по согласованности – вид инцидента, фиксирующий ошибки, связанные с полным или частичным несоответствием представленных цифровых данных установленному порядку представления и обозначения, отступлением от соответствующих требований или стандартов;

по целостности – вид инцидента, фиксирующий ошибки, связанные с наличием в представленных цифровых данных некорректных связей между цифровыми данными (записями и агрегатами цифровых данных);

прочие – вид инцидента, фиксирующий ошибки, не идентифицированные настоящими требованиями.

58. В рамках выявления ошибок в цифровых данных осуществляется автоматизированный форматно-логический контроль, подразумевающий проверку:

соответствия цифровых данных базовым свойствам атрибутов цифровых данных и дополнительным требованиям к значениям атрибутов цифровых данных, характеризующих объект описания, заданных в паспорте цифровых данных:

соответствия состава переданных цифровых данных запросу;

отсутствия незаполненных обязательных атрибутов – все атрибуты вида цифровых данных, относящиеся к категории обязательных, необходимо заполнить цифровыми данными;

отсутствия дублей в атрибутах, определенных в качестве идентификаторов, – в массиве цифровых данных необходимо устранить дубли идентификаторов, то есть две и более записи, содержащие идентичные идентификаторы вида цифровых данных;

своевременности предоставления цифровых данных по требованиям, установленным законодательством Республики Казахстан, подписке и запросу по цифровым данным.

59. При подтверждении организацией факта ошибки в цифровых данных пользователям, имеющим право доступа к цифровым данным, относящимся к виду цифровых данных, направляется уведомление о соответствующем инциденте.

В виде цифровых данных при установлении ошибки и наличии эталонных цифровых данных в уведомлении устанавливается требование о приостановлении гармонизации с такими цифровыми данными (в части значений) до устранения ошибки в цифровых данных.

60. Организация выявляет причину возникновения ошибки и принимает незамедлительные меры по ее устранению.

По результатам внесения исправлений в записи, связанных с устранением ошибок в цифровых данных, поставщик цифровых данных направляет уведомление пользователям, имеющим право доступа к цифровым данным, об устранении ошибки в цифровых данных и внесенных исправлениях в цифровых данные, о снятии ограничения по гармонизации цифровых данных.

При инициировании пользователем цифровых данных (заявителем) инцидента об ошибке цифровых данных результат решения инцидента направляется пользователю цифровых данных (заявителю).

При удовлетворенности результатом отработки инцидента пользователь цифровых данных закрывает инцидент, о чем делает отметку в журнале инцидентов.

Пользователем цифровых данных (заявитель) и поставщиком цифровых данных, не пришедшими к согласию, инцидент, связанный с выявленной ошибкой цифровых данных, разбирается на согласительном совещании с участием представителей пользователя цифровых данных, поставщика цифровых данных, центра, уполномоченного органа.

По результатам проведения согласительного совещания формируется протокол с перечнем решений по устранению инцидента.

Глава 4. Требования к доступу и распространению цифровых данных

61. С целью обеспечения эффективного информационного взаимодействия цифровых объектов организации проводят интеграцию цифровых объектов в соответствии с правилами интеграции цифровых объектов "цифрового правительства", утверждаемыми уполномоченным органом в сфере цифровизации, согласно пункту 3 статьи 83 Цифрового кодекса Республики Казахстан.

62. При осуществлении государственных функций и оказании вытекающих из них государственных услуг согласие государственных органов на доступ к цифровым

данным, содержащимся в цифровых объектах "цифрового правительства", не требуется

63. Организации обеспечивают доступ к цифровым данным для целей осуществления государственных функций и оказания государственных услуг на безвозмездной основе.

Доступ и распространение цифровых данных, отнесенных к конфиденциальной информации, осуществляются в соответствии с Законом Республики Казахстан "О персональных данных и их защите".

Глава 5. Требования к аналитике цифровых данных

64. Аналитика цифровых данных осуществляется организациями самостоятельно и (или) путем привлечения поставщиков.

Аналитика цифровых данных, отнесенных к конфиденциальной информации, осуществляется при условии их обезличивания организациями.

Аналитика цифровых данных допускается только при наличии утвержденной методологии расчетов по ее проведению.

65. При создании и внедрении аналитического дашборда организация:

1) формирует и утверждает паспорт кейса по форме, согласно приложению 3 к настоящим требованиям, по согласованию с уполномоченным органом, определяющим целесообразность создания и внедрения аналитического дашборда;

2) формирует и подписывает регламент взаимодействия SDU (далее – регламент взаимодействия) между цифровыми системами, необходимыми для создания и внедрения аналитических дашбордов (при необходимости).

66. Организации осуществляют закуп услуг по созданию, внедрению и сопровождению аналитических дашбордов в соответствии с законодательством Республики Казахстан о государственных закупках, в том числе у оператора.

67. Организации направляют оператору утвержденный паспорт кейса, договор оказания услуг по созданию, внедрению и сопровождению аналитических дашбордов, регламент взаимодействия между цифровыми системами, необходимыми для создания и внедрения аналитических дашбордов (при наличии).

68. Оператор после получения документов, указанных в пункте 70 настоящих требований, формирует и тестирует нулевые витрины цифровых данных, являющиеся хранилищем, куда поступают и хранятся цифровые данные в исходном коде без предварительной обработки, а также очистки, разрабатывает техническое задание для инженеров цифровых данных.

69. Оператор осуществляет подключение требуемых источников цифровых данных с настройкой периодичности обновления источников и витрин цифровых данных.

70. При необходимости оператор предоставляет доступ исполнителям по договору оказания услуг по созданию, внедрению и сопровождению аналитических дашбордов к инструментам SDU.

71. После получения доступа к инструментам SDU исполнитель по договору оказания услуг по созданию, внедрению и сопровождению аналитических дашбордов осуществляет формирование витрин цифровых данных не нулевого уровня и формирует аналитический дашборд.

72. После создания и внедрения аналитического дашборда организации обеспечивают его дальнейшее сопровождение.

73. В целях осуществления сбора, обработки, хранения, передачи цифровых данных для осуществления аналитики цифровых данных организации привлекают оператора.

Обезличивание цифровых данных производится оператором при невозможности его осуществления самостоятельно организацией.

С организациями, определенными оператором, заключается регламент взаимодействия с цифровым объектом организации.

Оператор в течение пяти рабочих дней запрашивает у организации описание таблиц, полей БД для сбора общих сведений об цифровой системе.

Оператор в течение пяти рабочих дней разрабатывает, согласовывает, утверждает и направляет организации регламент взаимодействия с цифровой системой организации.

Организация в течение пяти рабочих дней согласовывает и утверждает регламент взаимодействия.

При наличии цифровых данных на платформе "цифрового правительства" заключение регламента взаимодействия с организацией не требуется.

Согласование, обезличивание и передача цифровых данных происходят в следующих случаях:

1) оператор совместно с организацией определяет и согласовывает перечень цифровых данных, подлежащих обезличиванию;

2) оператор предоставляет организации разработанные алгоритмы (последовательность действий) для одностороннего шифрования без возможности обратного восстановления по типам БД и инструкцию по обезличиванию;

3) организация производит обезличивание цифровых данных и предоставляет цифровые данные оператору по согласованной с оператором структуре;

4) для организаций, не производящих обезличивание цифровых данных, оператор настраивает процедуру обезличивания через ETL, при этом в SDU хранятся только обезличенные цифровые данные;

5) оператор проверяет корректность цифровых данных, корректность обезличивания цифровых данных и загружает их в SDU.

Организации передают и предоставляют доступ оператору к цифровым данным и цифровым записям. Далее оператор через ETL производит работы по подключению,

преобразованию форматов и кодировок, выявлению и удалению ошибок и несоответствий в цифровых данных с целью улучшения их качества.

Оператор совместно с организациями внедряет техническое решение и подходы к репликации структуры цифровых данных из БД организаций в каталоге цифровых данных оператора, являющемся централизованным хранилищем метаданных для поиска и дальнейшего управления своими цифровыми данными:

- блочная репликация на уровне системы хранения цифровых данных;

- физическая репликация на уровне систем управления БД;

- логическая репликация на уровне систем управления БД.

Для выгрузки цифровых данных из БД организации осуществляют настройку сетевого доступа согласно регламенту взаимодействия.

Организации создают учетную запись (для SDU без прикрепления к определенному лицу оператора) пользователя в БД для чтения определенных цифровых данных, открывают доступ на сервере для серверов SDU по определенным портам.

Оператор согласовывает с уполномоченным органом сроки и объем предоставления цифровых данных, полученных из различных БД и объединенных между собой, согласно направленному заказчиком аналитики цифровых данных уполномоченному органу запросу по цифровым данным.

Оператор в течение 30 (тридцать) рабочих дней предоставляет цифровые данные, полученные из различных БД и объединенные между собой, согласно направленному заказчиком аналитики цифровых данных уполномоченному органу запросу по цифровым данным для последующей аналитики.

Собранные цифровые данные (детальные данные, обработанные данные, результаты аналитических решений) подлежат хранению и обновлению в SDU. Обновление цифровых данных осуществляется оператором в автоматическом режиме согласно регламенту взаимодействия.

Признак для определения среза обновленных цифровых данных предоставляется организацией.

При возникновении необходимости высокой частоты обновления цифровых данных оператор настраивает регламентное обновление посредством CDC. В свою очередь организация должна произвести технические работы для функционирования CDC.

Оператор предоставляет доступ заказчику аналитики цифровых данных к подготовленным обработанным цифровым данным для проверки на соответствие запрашиваемых цифровых данных.

Заказчик аналитики цифровых данных в течение пяти рабочих дней дает информацию оператору о результатах проверки. При отрицательных результатах, отсутствии и (или) недостаточности необходимых цифровых данных оператор осуществляет повторную обработку цифровых данных в сроки, установленные регламентом взаимодействия.

Положительные результаты проверки на соответствие запрашиваемых цифровых данных способствуют проведению аналитики цифровых данных, которая осуществляется заказчиком аналитики цифровых данных самостоятельно и (или) путем привлечения поставщика, за счет собственных финансовых средств.

Результаты аналитики, хранящиеся в SDU в обезличенном виде, передаются оператором также в обезличенном виде по согласованию с уполномоченным органом заинтересованным организациям на возмездной основе.

Глава 6. Требования к передаче и защите цифровых данных

74. В целях защиты цифровых данных организации обеспечивают:

определение степени необходимости защиты цифровых данных в зависимости от класса цифровых данных, который присваивается в соответствии с их масштабом, целостностью, критичностью и классификатором цифровых объектов;

сбор и анализ цифровых данных о состоянии кибербезопасности в организации;

оценку рисков и планирование мер по обработке рисков при возможной утечке (разглашении), искажении, удалении (потеря) цифровых данных;

реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение сотрудников, оперативную работу по осуществлению защитных мероприятий;

мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия;

соблюдение ЕТ и настоящих требований.

75. Обеспечение изготовления резервной копии государственных данных является обязательным для организаций.

Способ изготовления и хранения резервной копии, содержащей государственные цифровые данные, обеспечивает ее сохранность, целостность, конфиденциальность, актуальность, доступность хранимых на ней данных до изготовления следующей резервной копии.

Периодичность резервного копирования государственных цифровых данных устанавливается технической документацией на цифровой объект "цифрового правительства".

76. Цифровые данные, подвергнутые обезличиванию, рассматриваются в качестве информации об идентифицируемом объекте описания и защищаются в соответствии с особенностями, установленными законами Республики Казахстан.

В целях установления объекта описания идентификации учитываются способы (извлечение записей, относящихся к данному объекту описания), технологии, доступные на момент обработки цифровых данных, в отношении которых существует вероятность, что они будут использованы третьими лицами в целях прямой или косвенной идентификации объекта описания.

77. В целях разграничения ответственности и функций в сфере обеспечения кибербезопасности в организации создается подразделение кибербезопасности, являющееся структурным подразделением, обособленным от структурных подразделений, и (или) определяется лицо, ответственное за обеспечение кибербезопасности, установленной ЕТ и нормативными правовыми актами Республики Казахстан в области цифровизации.

78. Передача цифровых данных организациями через провайдеров цифровых данных, осуществляющих функцию передачи цифровых данных от одного лица к другому, осуществляется при соблюдении провайдерами требований настоящей главы.

При передаче цифровых данных организации обеспечивают:

идентификацию и аутентификацию участников обмена;

регистрацию и учет операций по передаче цифровых данных;

конфиденциальность и целостность цифровых данных, включая применение средств криптографической защиты информации, протоколов защищенной передачи, контроля целостности;

заключение договоров или соглашений, предусматривающих обязательство провайдеров цифровых данных по применению технических и технологических мер обеспечения кибербезопасности и сохранности передаваемых цифровых данных, соответствующих требованиям законодательства Республики Казахстан.

Глава 7. Требования к хранению, архивированию и уничтожению цифровых данных

79. Решение об отсутствии необходимости дальнейшего использования цифровых данных принимается организацией с уведомлением собственников и (или) владельцев цифровых объектов "цифрового правительства", с которыми интегрирован цифровой объект "цифрового правительства", центра о порядке и сроках прекращения использования цифровых данных.

80. Отсутствие необходимости дальнейшего использования цифровых данных влечет изменение сведений в каталоге.

81. Срок хранения цифровых данных определяется датой достижения целей их сбора и обработки.

82. Цифровые данные, использование которых прекратилось, подлежат архивированию и передаче в архив в соответствии с законодательством Республики Казахстан.

83. По истечении срока хранения цифровые данные подлежат уничтожению в соответствии с законодательством Республики Казахстан.

84. Организации в целях обеспечения актуализации реестра аналитических дашбордов:

1) размещают описание аналитического дашборда на архитектурном портале цифровых объектов государства согласно приложению 4 к настоящим требованиям;

2) обеспечивают актуальность, достоверность и полноту информации о аналитических дашбордах;

3) при выводе аналитического дашборда из эксплуатации и (или) создании нового аналитического дашборда в течение 3 (три) рабочих дней уведомляют посредством архитектурного портала цифровых объектов государства о необходимости удаления и (или) добавления аналитического дашборда в реестр аналитических дашбордов;

4) осуществляют мониторинг работоспособности и доступности аналитических дашбордов, находящихся в их зоне ответственности;

5) посредством официального письма уведомляют уполномоченный орган о плановых работах или временной недоступности аналитического дашборда.

85. Организации обеспечивают:

1) подготовку библиотеки данных в машиночитаемой форме в целях обучения моделей искусственного интеллекта;

2) составление паспорта библиотеки данных согласно приложению 5 к настоящим требованиям;

3) формирование метаданных;

4) формирование контрольной суммы библиотеки данных;

5) первичную валидацию качества библиотеки данных.

86. Цифровые данные, использование которых противоречит ограничениям доступа, согласию субъектов и (или) лицензионным условиям, не включаются в библиотеки данных.

При необходимости включения в библиотеку данных персональных данных и (или) конфиденциальной информации организации обеспечивают их обезличивание до передачи оператору.

При невозможности осуществления обезличивания данных самостоятельно организацией обезличивание производится оператором.

Метод обезличивания и перечень атрибутов библиотеки данных, подлежащих обезличиванию, отражаются в паспорте библиотеки данных.

87. Подключение к данным, необходимым для формирования библиотеки данных осуществляется посредством SDU с дальнейшим предоставлением доступа к ним оператором на возмездной основе оператору НПИИ.

88. Оператор НПИИ при размещении библиотеки данных осуществляет проверку контрольной суммы и соответствие библиотеки данных сведениям паспорта библиотеки данных.

При выявленных несоответствиях оператор НПИИ осуществляет возврат библиотеки данных организации на доработку с указанием выявленных несоответствий.

89. Организация:

1) назначает лицо, ответственное за формирование и качество библиотеки данных;

2) управляет версионированием библиотеки данных;

3) осуществляет актуализацию библиотеки данных, паспорта библиотеки данных, метаданных и контрольной суммы при изменении структуры библиотеки данных, источников формирования библиотеки данных, формул расчета показателей параметров, хранимых в библиотеке данных.

Приложение 1
к требованиям по управлению
цифровыми данными
Форма

Паспорт цифровых данных цифровых объектов

1. Общая часть

1) наименование организации:

указывается полное наименование организации;

к примеру: государственное учреждение "Министерство юстиции Республики Казахстан";

2) наименование цифрового объекта, осуществляющего сбор и обработку цифровых данных:

указывается полное наименование цифрового объекта, осуществляющего сбор и обработку цифровых данных (так, как оно закреплено в соответствующих нормативных правовых актах (далее – НПА), при наличии);

к примеру: национальный реестр индивидуальных идентификационных номеров;

3) уровень межведомственного использования цифровых данных:

указывается уровень межведомственного использования цифровых данных выбором одной из следующих возможных альтернатив: республиканский; местный; цифровые данные на межведомственном уровне не используются;

4) способ ведения:

указывается один из следующих способов ведения: в бумажном виде (указывается для данных, не переведенных в электронный вид); в электронном виде (указывается для данных, представленных в электронном виде); комбинированный (указывается для данных, которые частично переведены в электронный вид);

5) форма цифровых данных:

указываются одна или несколько из следующих форм цифровых данных: первичные цифровые данные; агрегированные цифровые данные;

6) доступность цифровых данных:

указываются уровни доступности цифровых данных: ограниченный доступ (указывается при наличии персональных данных, коммерческой тайны, служебной тайны и данных, охраняемых законами Республики Казахстан); доступ без ограничений

(указывается для открытых данных) (при разном уровне доступа к отдельным частям цифровых данных в данной строке проставляются оба перечисленных выше варианта с детализацией сведений);

7) пользователи цифровых данных согласно НПА:

указывается полный перечень наименований пользователей цифровых данных согласно НПА, если круг пользователей определен НПА, получивших интеграции;

8) источник цифровых данных согласно НПА:

указывается согласно НПА полный перечень цифрового объекта.

В отсутствии НПА указывается "Не определено НПА".

9) источники цифровых данных фактические:

указывается фактический перечень цифрового объекта.

Если состав фактических источников цифровых данных совпадает с составом источников цифровых данных согласно НПА, указывается, что перечень фактических источников совпадает с предусмотренным НПА.

10) объект описания:

указываются объекты описания, к которым относятся: физические лица; юридические лица; имущество, включая наличные деньги и документарные ценные бумаги, безналичные денежные средства, бездокументарные ценные бумаги, имущественные права; результаты работ и оказания услуг; охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага;

11) периодичность обновления:

указывается один из следующих вариантов периодичности обновления цифровых данных: периодичность обновления не установлена; обновление по мере необходимости; обновление по мере поступления цифровых данных; непрерывное обновление (поток цифровых данных); периодичность обновления установлена НПА (указать наименование НПА и периодичность обновления);

12) график обновления:

указываются в зависимости от особенностей обновления цифровых данных: заданный интервал времени с момента последнего обновления; перечень плановых календарных дат; реквизиты НПА, регламентирующего график обновления (при отсутствии графика обновления цифровых данных указывается "Не определен");

13) порядок обновления:

указываются порядок обновления цифровых данных и его особенности (например, необходимость подписания/согласования НПА) (если порядок установлен НПА, то указывается наименование такого НПА);

14) перечень НПА, на основании которого создан цифровой объект, осуществляющий сбор и обработку цифровых данных:

указывается перечень НПА, регламентирующих сбор и обработку цифровых данных (положения, регламенты информационного взаимодействия, раздел не заполняется, если цифровые данные ведутся в бумажном виде);

15) перечень НПА, регламентирующих сбор и обработку цифровых данных:

указывается перечень НПА, содержащих функции ведения объекта учета или цифровых данных организацией;

16) перечень НПА, регламентирующих внесение и потребление цифровых данных, ограничение и разделение доступа к цифровым данным:

указывается перечень НПА, определяющих правила функционирования, внесения или передачи цифровых данных, правила доступа к цифровым данным и использования этих цифровых данных, правила разграничения доступа к цифровым данным;

17) класс цифровых данных;

18) дата создания – дата создания паспорта цифровых данных.

2. Описание жизненного цикла цифровых данных:

1) создание сведений об объекте учета:

указывается порядок первоначального формирования цифровых данных об объекте учета, при этом указывается: являются ли цифровые данные первичными или формируются на основании цифровых данных, предоставляемых из не утвержденных источников (если при формировании записи об объекте учета используются сведения из разных источников информации, то необходимо перечислить их с указанием соответствующих НПА);

2) использование сведений об объекте учета:

указываются сведения о порядке использования цифровых данных об объекте учета, являются ли цифровые данные об объекте учета (все или их часть) первоисточником; существующие механизмы передачи цифровых данных (например, файловая передача цифровых данных; передача цифровых данных посредством интеграционного сервиса); используют ли цифровые данные об объекте учета представители бизнеса (с описанием, кто и для чего использует цифровые данные); уровень доступности цифровых данных (существуют ли правовые ограничения на использование цифровых данных);

3) изменение объекта учета, удаление сведений об объекте учета – указание или описание этапа нахождения жизненного цикла цифровых данных объекта учета:

создание (сбор) цифровых данных;

хранение цифровых данных и их ведение;

использование цифровых данных;

управление цифровыми данными;

архивирование цифровых данных (или их уничтожение).

3. Описание структуры цифровых данных

порядковый номер атрибута данных в таблице (id);

наименование цифрового объекта (information_system_name);
системное наименование базы данных (bd_name);
наименование схемы в базе данных (schema_name);
наименование таблицы базы данных (table_name);
описание назначения таблицы базы данных (table_description);
указание типа таблицы базы данных (table_type);
порядковый номер столбца в таблице базы данных (column_id);
наименование столбца в таблице базы данных (column_name);
тип данных столбца в таблице базы данных (column_type);
назначение столбца в таблице базы данных (column_description);
ссылка на другую таблицу базы данных, при наличии, (reference_tbl_clmn);
ограничение столбца в таблице базы данных (flk);
вид ключа столбца в таблице базы данных (clmn_key_type);
семантический словарь тегов (teg);
мастер данные (isMD);
государственная услуга (isGosService).

Приложение 2
к требованиям по управлению
цифровыми данными
Форма

Описание неоцифрованных данных

1. Вид объекта неоцифрованных данных (например: субъект, объект, документ).
2. Наименование сущности субъекта или объекта неоцифрованных данных (например: пассажир, перевозчик, пациент, врач, пенсионер, здание, земельный участок, транспортное средство).
3. Описание объекта неоцифрованных данных (указать наименование нормативных правовых актов, регламентирующих сбор и обработку цифровых данных).
4. Наименование атрибута (например: фамилия, имя, отчество (при наличии), дата рождения, номер документа, номер транспорта).
5. Национальная справочная информация.

Приложение 3
к требованиям по управлению
цифровыми данными
Форма

Паспорт кейса

1. Организация _____.
2. Название кейса _____.
3. Постановка цели _____.

4. Описание _____.

5. На какие вопросы должен отвечать дашборд _____.

6. Показатели (с учетом разрезности, методик/формул формирования, источника):

6.1. Описание показателя:

№ п/п	Показатель	Разрезность	Источник	Периодичность обновления
-------	------------	-------------	----------	--------------------------

6.2. Методика расчета показателя _____.

7. Описание необходимой аналитики: (описательный анализ, анализ "что-если", прогнозный анализ) _____.

8. KPI дашборда (ключевые показатели эффективности (KPI), которые необходимо отслеживать) _____.

9. Планируемые графики для отображения результата (согласованный макет графика) _____.

10. Согласованные допущения при реализации кейса _____.

11. Согласование сторон _____.

Приложение 4
к требованиям по управлению
цифровыми данными
Форма

Описание аналитического дашборда на архитектурном портале цифровых объектов государства

1. Наименование дашборда: _____;
(краткое и понятное название)

2. Цель/назначение: _____;

(например: мониторинг ключевых показателей региона, контроль исполнения бюджета и так далее)

3. Государственный орган/организация: _____;

(владелец/разработчик дашборда)

4. Ответственное подразделение и контактное лицо: _____;

(фамилия, имя, отчество (при наличии), должность, e-mail, телефон)

5. Адрес сайта или ссылка на ведомственную платформу: _____;

6. Контур: _____;

(единая транспортная среда государственных органов /интернет)

7. Частота обновления данных: _____
—;
(ежедневно / еженедельно / ежеквартально/ раз в полгода/ раз в год/ по мере поступления данных и так далее)
8. Перечень источников: _____
—;
(наименование цифровой системы, базы данных)
9. Перечень показателей: _____
—;
10. Метод обновления данных: _____
—;
(автоматическое / полуавтоматическое / вручную)
11. Инструмент визуализации _____
— .

Приложение 5
к требованиям по управлению
цифровыми данными
Форма

Паспорт библиотеки данных

1. Общие положения
 - 1) назначение документа;
 - 2) область применения (обучение модели, дообучение модели, поиск по базе, тестирование, оценка качества, эксплуатация);
 - 3) термины и определения;
 - 4) наименование и версия библиотеки данных;
 - 5) наименование владельца библиотеки данных;
 - 6) наименование поставщика библиотеки данных и его структурного подразделения, фактически формирующего библиотеку данных;
 - 7) наименование организации, размещающей библиотеку данных;
 - 8) наименование организации, осуществляющей разработку цифрового объекта, взаимодействующего с библиотекой данных;
 - 9) основание формирования библиотеки данных (наименование и реквизиты нормативного правового акта, поручения, договора, протокола, письма);
 - 10) сведения об ответственных лицах со стороны владельца библиотеки данных, включающие:
 - фамилию, имя, отчество (при наличии) менеджера по данным;
 - фамилию, имя, отчество (при наличии) ответственного за качество данных;
 - фамилию, имя, отчество (при наличии) ответственного за кибербезопасность;

фамилию, имя, отчество (при наличии), должность, подразделение, контакты сотрудника, реализующего извлечение, интеграцию данных;

11) сведения о лицах, осуществляющих согласование паспорта библиотеки данных со стороны владельца библиотеки данных, включающие:

фамилию, имя, отчество (при наличии);

должность;

дату согласования;

реквизиты документа согласования.

2. Цели и сценарии использования библиотеки данных

1) наименование компонента, использующего библиотеку данных (система искусственного интеллекта, платформенный программный продукт национальной платформы искусственного интеллекта, модель искусственного интеллекта, модуль формирования базы знаний, модуль классификации, модуль генерации документов, аналитический модуль и тому подобное);

2) цели использования библиотеки данных (обучение, дообучение, тестирование, оценка, эксплуатация, формирование базы знаний, формирование эталонного набора данных);

3) ключевые сценарии использования библиотеки данных (не менее 3 (три), не более 10 (десять)).

3. Состав данных и классификация

1) типы данных (структурированные данные (таблицы или витрины данных), текстовые данные; неструктурированные данные (сканированные документы, изображения, аудио), национальная справочная информация, эталонный набор данных) ;

2) объем и период охвата формирования библиотеки данных;

3) язык документов библиотеки данных.

4. Источники и происхождение данных

1) перечень источников данных, включая сведения:

наименование цифровой системы, реестра, хранилища, архива;

наименование владельца источника данных;

правовое основание владения данными;

тип данных;

способ извлечения данных (прикладной программный интерфейс (далее - API), пакетная загрузка данных (далее - ETL), потоковая передача изменений данных (далее - CDC), выгрузка);

периодичность обновления;

2) ограничения по источникам, связанные с запретом на использование данных, выгрузке данных, исключению атрибутов или их обезличиванию;

3) наименование первичного эталонного источника;

4) ожидаемый корректный результат для каждого элемента эталонного набора данных.

5. Форматы данных

- 1) перечень форматов текстовых данных;
- 2) перечень форматов неструктурированных данных;
- 3) перечень форматов структурированных данных.

6. Описание структуры данных и метаданные

- 1) схема библиотеки данных включает:

наименование таблицы;

назначение таблицы;

вид таблицы (основная, справочная, журнал событий, витрина данных);

тип таблицы (содержит первичный или внешний ключ);

периодичность обновления;

- 2) описание структуры таблицы включает:

наименование таблицы;

наименование поля таблицы;

тип базы данных;

признак типа формата данных (числовой, текстовый, категория, дата и время, логический, географический);

обязательность наличия данных в поле таблицы (ограничение Not Null);

принимаемые допустимые значения;

наименование ограничения, определяющего первичный или внешний ключ;

разрешение на дальнейшее использование данных оператором национальной платформы искусственного интеллекта для целей формирования иных библиотек данных (да или нет);

- 3) описание структуры метаданных включает:

уникальный идентификатор документа;

наименование источника данных;

вид документа;

язык документа;

заголовок страницы, описывающей контент документа;

дату создания или актуализации документа;

статус документа (утвержденный, утратил силу, проект);

контрольную сумму документа;

сведения о наличии персональных данных в документе или сведений конфиденциального характера;

текстовую информацию документа.

7. Описание порядка подготовки данных (ETL, CDC, очистка, преобразование)

- 1) описание маршрута данных в последовательности:

- источник данных;
 - способ извлечения;
 - зона приема данных (зона для временного хранения данных перед их обработкой или нулевая витрина данных);
 - способ преобразования, очистки;
 - наименование витрины или каталога;
 - наименование компонента, использующего библиотеку данных;
- 2) описание правил преобразования (нормализация форматов дат или кодировок, правила удаления дублей, правила обработки пропусков, правила сопоставления с национальной справочной информацией, правила исключения запрещенных атрибутов) ;
- 3) описание механизма определения изменения данных.

8. Качество и механизмы контроля качества данных

- 1) описание перечня применимых критериев качества (точность, полнота, взаимосвязанность, сопоставимость, актуальность, уникальность, достоверность, своевременность);
- 2) описание проверок для реализации форматно-логического контроля данных (заполненность обязательных атрибутов по ограничению Not Null, совпадение типов данных, диапазонов значений данных, применяемых масок, отсутствие дублирующих значений ключей и идентификаторов, корректность связей между таблицами по значениям первичного и внешних ключей, корректность допустимых значений в национальной справочной информации, соблюдение сроков обновлений);
- 3) описание результатов проверки качества данных, включающее:
- объем данных;
 - долю пропусков по обязательным полям (в процентах);
 - долю выявленных дублированных данных (в процентах);
 - количество нарушений форматно-логического контроля;
 - перечень критичных дефектов;
- 4) описание порядка обработки дефектов качества, включающее:
- способ фиксации инцидентов;
 - сроки реакции на выявленный инцидент;
 - фамилию, имя, отчество (при наличии) ответственных за обработку инцидента;
 - порядок повторной передачи исправленных данных для формирования библиотеки данных.

9. Эталонный набор данных для тестирования библиотеки данных

- 1) описание эталонного набора данных, включающее:
- назначение эталонного набора данных;
 - сценарии использования эталонного набора данных;
 - объем эталонного набора данных;

покрытие;

2) описание формата эталонного набора данных, включающее:

идентификатор эталонного набора данных;

сценарий использования;

вид входных данных (запрос, документ, набор полей);

ожидаемый корректный результат;

правила прохождения;

источник эталонного набора данных.

10. Описание механизмов защиты данных

1) описание режима доступа к данным и ролей доступа (открытый или ограниченный);

2) описание наличия конфиденциальных и (или) персональных данных, иных ограничений, связанных с их обработкой;

3) описание способа обезличивания данных (при необходимости), включающее:

наименование атрибута, подлежащего обезличиванию;

описание метода (маскирование, хэширование, агрегация, удаление);

места обезличивания;

способы и результаты контроля корректности обезличивания;

4) описание журналирования событий, включающее:

тип события, подлежащего журналированию (доступ, изменение);

срок и место хранения журналов событий.

11. Порядок предоставления и формат поставки данных для формирования библиотеки данных

1) описание способа предоставления данных (API, ETL, CDC, защищенная файловая передача, база данных со статусом "только для чтения);

2) описание комплекта поставки данных, включающее сведения о:

объеме и формате данных;

наличии метаданных;

наличии описания результатов проверок для реализации форматно-логического контроля данных эталонного набора данных (при наличии требований к оценке качества);

контрольных суммах переданных файлов с данными или выгрузок данных;

3) описание периодичности поставки данных и параметры SLA, включающие:

частоту (периодичность) поставки данных;

допустимую задержку поставки данных,

время окна обслуживания.

