

Регламентация резервного копирования и восстановления документов

На вопрос читателей отвечает начальник Управления правового обеспечения и международного взаимодействия Федеральной службы по аккредитации **Михаил Сергеевич Пигалицын**.

Вопрос: *Критерии аккредитации устанавливают требование о наличии в документах системы менеджмента качества органов по оценке соответствия системы управления документацией (правил документооборота), включающей правила резервного копирования и восстановления документов. Как Росаккредитация трактует понятие «резервное копирование» и что подлежит резервному копированию?*

Ответ: В законодательстве Российской Федерации об аккредитации в национальной системе аккредитации определение понятия «резервное копирование» отсутствует. Рассмотрим этот вопрос, опираясь на системное толкование положений Критериев аккредитации¹.

Ст. 13 № 412-ФЗ² обязывает аккредитованные лица соблюдать критерии аккредитации при осуществлении своей деятельности. Одним из таких критериев, независимо от типа аккредитованного лица, является наличие в системе менеджмента качества системы управления документацией (правил документооборота), включающей помимо прочего правила резервного копирования и восстановления документов (пп. 4.8, 24.6, 29.8, 46.7 Критериев аккредитации). В основе аккредитации лежат международные стандарты, требующие от органов по сертификации продукции/услуг соответствия ГОСТ Р ИСО/МЭК 17065–2012³ (согласно п. 3 Критериев аккредитации).

Лаборатории должны следовать требованиям ГОСТ ISO/IEC 17025–2019⁴ (п. 21 Критериев аккредитации), а органы инспекции — ГОСТ Р ИСО/МЭК 17020–2012⁵ (п. 28 Критериев аккредитации). Все упомянутые стандарты подчеркивают необходимость наличия у аккредитованных лиц надежной системы управления информацией, охватывающей все этапы: от сбора и обработки данных до представления результатов, их безопасного хранения и копирования.

Важно подчеркнуть, что Критерии аккредитации не регламентируют конкретные способы обеспечения резервного копирования, предоставляя заявителю/аккредитованному лицу самостоятельность в выборе решений. Перечень документов и записей, подлежащих резервному копированию, заявитель/аккредитованное лицо определяет самостоятельно и фиксирует в документах системы менеджмента качества. Практическая реализация резервного копирования подразумевает создание копий критически важных данных и их хранение в отдельном безопасном месте. Это может быть физический носитель, такой как внешний жёсткий диск или сетевой накопитель, либо виртуальное хранилище в облаке.

Процедура восстановления данных из резервной копии должна чётко документироваться и регулярно тестироваться. Это гарантирует, что в случае потери или повреждения данных их можно будет быстро и эффективно восстановить.

1 Критерии аккредитации и перечень документов и сведений, подтверждающих соответствие заявителя, аккредитованного лица критериям аккредитации, утверждены приказом Минэкономразвития России от 24.10.2020 № 707.

2 Федеральный закон от 28.12.2013 № 412–ФЗ «Об аккредитации в национальной системе аккредитации».

3 ГОСТ Р ИСО/МЭК 17065–2012 «Оценка соответствия. Требования к органам по сертификации продукции, процессов и услуг» введён в действие приказом Росстандарта от 21.12.2012 № 1941-ст.

4 ГОСТ ISO/IEC 17025–2019 «Общие требования к компетентности испытательных и калибровочных лабораторий» приказом Росстандарта от 15.07.2019 № 385-ст введён в действие в качестве национального стандарта с 01.09.2019.

5 ГОСТ Р ИСО/МЭК 17020–2012 «Оценка соответствия. Требования к работе различных типов органов инспекции» введён в действие приказом Росстандарта от 29.11.2012 № 1673-ст.

В документации системы менеджмента качества необходимо установить сроки создания резервных копий, а также периодичность проверки их работоспособности.

Таким образом, заявители/аккредитованные лица должны самостоятельно определить пере-

чень подлежащих резервному копированию документов и записей, включая документы, создаваемые органами по оценке соответствия в процессе сертификации, отчёты (протоколы) испытаний, протоколы или акты инспекции, но не ограничиваясь ими.

Комментарий издателя

Резервное копирование — это процесс создания копии данных, важной информации или всей документации организации для восстановления в случае потери, повреждения или недоступности оригинальных данных. Это фундаментальный аспект стратегии защиты данных, который обеспечивает возможность оперативного восстановления рабочих процессов после различных инцидентов.

Существует множество причин, по которым резервное копирование необходимо, например:

- **защита от потери данных** — при человеческих ошибках, аппаратных сбоях, вирусных атаках, стихийных бедствиях и в иных непредвиденных случаях резервные копии позволяют восстановить утраченные данные и избежать катастрофических последствий для организации;
- **восстановление после сбоев** — в случае аварии или сбоя системы резервные копии позволяют быстро восстановить работоспособность системы и минимизировать время простоя, что особенно актуально в отношении критически важных приложений и сервисов;
- **сохранение данных** — в некоторых случаях, когда данные необходимо сохранять в течение длительного времени в соответствии с требованиями законодательства или регуляторных органов, резервные копии обеспечивают их надежное хранение на протяжении всего необходимого периода.

В современном мире, где информация/данные являются одним из самых ценных активов любой организации, обеспечение их сохранности и доступности становится важнейшей задачей. Непрерывность бизнес-процессов, соответствие нормативным требованиям и поддержание репутации компании напрямую зависят от эффективности системы резервного копирования и восстановления данных. Именно поэтому международные стандарты, устанавливающие требования к органам по оценке соответствия, такие как *ISO/IEC 17020*, *17025* и *17065*, предусматривают резервное копирование, направленное на гарантированное восстановление данных в непредвиденных обстоятельствах.

Требования к резервному копированию для восстановления данных установлены международными стандартами *ISO/IEC 17020*, *17025*, *17065*.

- ***ISO/IEC 17020*** акцентирует внимание на беспристрастности, компетентности и последовательности в деятельности органов инспекции. Резервное копирование данных, включая результаты оценки, протоколы и записи, является обязательным элементом обеспечения целостности и доступности информации, необходимой для подтверждения беспристрастности и соответствия требованиям.

ГОСТ Р ИСО/МЭК 17020 (п. 8.4)

8.4.1 Орган инспекции должен разрабатывать процедуры для определения средств управления, требуемых **для идентификации, хранения, защиты, восстановления, сохранения и изъятия записей**, относящихся к выполнению требований настоящего международного стандарта.

8.4.2 Орган инспекции должен разрабатывать процедуры для сохранения записей на период времени, согласующийся с его договорными и правовыми обязательствами. Доступ к таким записям должен отвечать мерам по обеспечению конфиденциальности.

- **ISO/IEC 17025** определяет требования к компетентности испытательных и калибровочных лабораторий. Лабораториям жизненно важно иметь надёжную систему резервного копирования для сохранения данных исследований (испытаний) и измерений, результатов калибровки и другой важной информации, которая может потребоваться для повторного анализа, аудита или воспроизведения результатов.

ГОСТ ISO/IEC 17025 (п. 8.4)

8.4.1 Лаборатория должна вести и сохранять разборчивые записи с целью подтверждения соблюдения требований настоящего стандарта.

8.4.2 Лаборатория должна осуществлять управление, необходимое **для идентификации, хранения, защиты, резервного копирования, архивирования, поиска, срока хранения и уничтожения своих записей**. Лаборатория должна сохранять записи в течение периода, установленного договорными обязательствами. Доступ к данным записям должен соответствовать обязательствам в области конфиденциальности, и записи должны быть легкодоступными.

- **ISO/IEC 17065** регламентирует деятельность органов по сертификации продукции, процессов и услуг. Резервное копирование здесь обусловлено необходимостью гарантировать сохранность записей о выданных сертификатах, аудиторских отчётах и другой документации, подтверждающей соответствие сертифицированной продукции, процессов и услуг установленным требованиям.

ГОСТ Р ИСО/МЭК 17065 (п. 8.4)

8.4.1 Орган по сертификации должен разработать процедуры определения средств управления, необходимых **для идентификации, хранения, защиты, поиска, определения сроков хранения и уничтожения записей**, имеющих отношение к выполнению требований настоящего стандарта.

8.4.2 Органу по сертификации следует разработать процедуры сохранения записей (см. 7.12) в течение периода, определяемого контрактными и правовыми обязательствами. Доступ к этим записям должен определяться мерами по соблюдению конфиденциальности.

Несмотря на то, что в стандартах нет детализированных инструкций по реализации резервного копирования, они задают общие принципы, которым должна соответствовать организация. Эти принципы можно свести к следующим ключевым:

- **идентификация критически важных данных**, прежде всего тех, потеря которых может привести к серьезным последствиям для деятельности организации (данные о результатах оценки соответствия, исследований, финансовая информация, проектная документация и т. д.);
- **разработка и внедрение организацией процедуры резервного копирования**, в которой будут определены его частота, методы, место хранения резервных копий, процедуры восстановления данных и ответственные лица;
- **регулярное тестирование процедур восстановления** необходимо проводить, чтобы убедиться, что резервные копии не повреждены и что процесс восстановления проходит успешно в установленные сроки;
- **обеспечение безопасности резервных копий** — защищённость от несанкционированного доступа, повреждения или уничтожения может быть достигнута за счёт использования шифрования, контроля доступа и защиты мест хранения резервных копий;
- **ведение документации** обеспечит все аспекты системы резервного копирования, включая правила и процедуры, результаты оценки соответствия и любые изменения. Документирование необходимо для обеспечения прозрачности, подотчетности и возможности проведения аудита.

Реализация требований, вытекающих из стандартов, требует комплексного подхода и выбора подходящих технологий. Организации могут выбирать между различными решениями для резервного копирования, включая внешние жесткие диски, сетевые накопители, облачные сервисы и гибридные решения. Выбор конкретной технологии зависит от потребностей организации, объёма данных, бюджета и требований к скорости восстановления.