Электронный документооборот – это требование настоящего момента, позволяет не только тратить на ведение документации и записей как можно меньше времени, но и отслеживать все этапы работы ИЛ. Для современных лабораторий с автоматическими измерительными системами такой подход вообще единственно возможный (допустим, анализ 100 проб в день) и такие ИЛ уже есть в нашей стране.

Однако, подход еще только развивается, и нет единого понимания, какие конкретно требования по «степени защищенности» следует предъявлять к электронному документообороту ИЛ, особенно когда в организациях сохраняется ведение записей на бумажных носителях, и система документооборота остается смешанной.

Содержание.

1. Требования стандартов
2. Существующие системы и схемы электронного документооборота в ИЛ
3. Обеспечение аутентичности первичных данных измерений, обработки результатов испытаний и отчетных документов для систем электронного документооборота в ИЛ
4. Пути решения проблемы обеспечения аутентичности данных для частично компьютеризированных систем документооборота в ИЛ
5. Выводы

**1) Требования стандартов**

Основные требования содержатся в ГОСТ ИСО/МЭК 17025-2009: «Общие требования к компетентности испытательных и калибровочных лабораторий».

4.13.1.2. Записи должны быть удобочитаемыми, легкодоступными и находиться в местах, обеспечивающих их защиту от повреждений, порчи и утери. Должны быть установлены сроки хранения записей.

**Примечание. Записи могут храниться на любом носителе, например, бумажном или электронном**

4.13.1.3. Все записи должны храниться в условиях безопасности и конфиденциальности.

4.13.1.4. Лаборатория должна иметь **процедуры для защиты и восстановления записей на электронных носителях, а также для предупреждения несанкционированного доступа или внесения изменений в них**.

4.13.2.3. Если в записях обнаруживаются ошибки, то каждая ошибка должна быть перечеркнута и рядом должно быть написано правильное значение. Все подобные изменения должны быть подписаны или завизированы лицом, внесшим изменение. **Если записи хранятся в электронном виде, то должны быть приняты меры, чтобы избежать потери или изменения первоначальных данных.**

4.3.3.4. Должны быть установлены процедуры для описания внесения и управления изменениями в документах, хранящихся в компьютерных системах.

5.4.7.2. Если используют компьютеры или автоматизированное оборудование для сбора, обработки, регистрации, отчетности, хранения или поиска данных испытаний и калибровки, то лаборатория должна гарантировать, что:

a) разработанное пользователем компьютерное программное обеспечение достаточно подробно задокументировано и должным образом оценено как пригодное для применения;

b) **разработаны и внедрены процедуры защиты данных; эти процедуры должны включать в себя, но не ограничиваться этим, целостность и конфиденциальность ввода или сбора данных, хранения данных, передачи данных и обработки данных**;

c) для должного функционирования обеспечен технический уход за компьютерами и автоматизированным оборудованием и для них созданы соответствующие условия окружающей среды и выполнены работы, необходимые для поддержания точности данных испытаний и калибровки.

Примечание. Коммерческое готовое программное обеспечение (например, обработка тестов, база данных и статистические программы), обычно используемое в обозначенных рамках его применения, может считаться достаточно оцененным. Однако конфигурацию/модификацию программного обеспечения, используемого в лаборатории, следует оценить [см. [5.4.7.2, перечисление a)](file:///D:\ASA\ИЛ%2017025\Аккр%20ИЛ\Подготовка%202015\Подготовка%20Лена\Подготовка%202015\Рук%20по%20кач%202015%20по%20критериям\ГОСТ%20ИСО-МЭК%2017025-2009.rtf#Par397)].

Есть еще стандарты по ведению электронных документов

ГОСТ Р 54989-2012 /ISO/TR 18492:2005 «Обеспечение долговременной сохранности электронных документов», использует понятие «**аутентичный электронный документ** – электронный документ, точность, надежность и целостность которого сохраняется с течением времени»

п.5.2.7.4. Управление доступом и защита документов.

**«Электронные документы, сохраняемые на перезаписываемом носителе, можно модифицировать, не оставив каких-либо следов**…Ввиду этого, организациям, стремящимся обеспечить аутентичность электронных документов во времени, следует разработать соответствующую политику, практику и технические меры контроля и управления. Примерами широко используемых технических мер являются:

- использование магнитных или оптических носителей однократной записи типа WORM;

- применение защищенной клиент-серверной архитектуры, которую можно использовать для блокирования непосредственного доступа к электронным документам, и которая в итоге позволяет организовать доступ «только на чтение»;

- использование циклического избыточного кода CRC (контрольных сумм CRC) – распространенный метод обеспечения надежности электронной передачи данных. Контрольные суммы CRC особенно полезны для подтверждения того, что никакие изменения не были внесены в электронные документы с момента их первоначального сохранения;

- применение односторонних хэш-функций (например, SHA-1), использующих алгоритм, позволяющий сжать электронные документы до фиксированного числа битов. Эти биты фактически являются уникальным «дактилоскопическим отпечатком» соответствующих документов, их впоследствии можно использовать для доказательства того, что информация не была изменена.»

ГОСТ 31887-2012 «Применение принципов надлежащей лабораторной практики к компьютеризированным системам». Этот стандарт идентичен международному стандарту 1995 г, ничего существенного не предлагает, только:

п.3.2.6 а) Физическая безопасность - ограничение доступа к компьютерному оборудованию;

б) Логическая безопасность – введение уникального идентификатора пользователя с соответствующим паролем.

Для оборудования, использующего программное обеспечение требования, требования определены четко, например:

ГОСТ Р 53228-2008 «Весы неавтоматического действия. Часть 1. Метрологические и технические требования».

В разделе требований к электронным весам с программным управлением указано:

«5.5.2.2 Законодательно контролируемое программное обеспечение ПК, т.е. программные средства, отвечающие за хранение и передачу измеряемых характеристик, данных измерений… должно быть надлежащим образом защищено от случайных или намеренных изменений….

Законодательно контролируемое программное обеспечение со всеми данными, параметрами… считают защищенным в достаточной мере, если его невозможно изменить с помощью обычных программных средств. Например, [таких как]…все виды текстовых редакторов…

Приемлемое решение [для обеспечения защиты]: Вычисление контрольной суммы по машинному коду… программного обеспечения во время выполнения работы и ее отображение на показывающем устройстве по ручной команде. Данная контрольная сумма уникальна для законодательно контролируемого программного обеспечения, ее можно сравнить с контрольной суммой, определенной при утверждении типа [весов]».

«5.5.3.3 Хранящиеся законодательно контролируемые данные должны быть соответствующим образом защищены от случайных или преднамеренных изменений.

Примеры приемлемых решений: а) Для защиты данных от случайных изменений в процессе передачи считают достаточным проведение простого контроля по четности.»

Из анализа стандартов следует, что устанавливаются три основных принципа защиты данных:

I – **сохранность** (в физическом смысле, должно быть обеспечено надлежащее хранение и дублирование для возможности восстановления);

II – **конфиденциальность** (ограничение доступа для неуполномоченных лиц при хранении и передаче);

III – **аутентичность**, или целостность данных (гарантия того, что данные невозможно изменить, а если это произошло, то появляются объективные свидетельства такого изменения).

Что касается I и II принципов, то все ИЛ вполне могут обеспечить их выполнение (дублирование записей любыми доступными способами, ограничение на вход в помещения, пароли для входа в компьютерные системы, доступность файлов регистрации данных операторам только на время проведения анализа одной серии проб и т.д.)

Следует иметь в виду, что **меры, обеспечивающие сохранность и конфиденциальность, вовсе не обеспечивают аутентичность данных**, при этом если даже вся система электронного документооборота имеет квалифицированную защиту, но есть одно слабое незащищенное звено, то всегда будет возможность поставить под сомнение аутентичность исходных данных и результатов испытаний.

**2) Существующие системы и схемы электронного документооборота в ИЛ**

Организация документооборота в лабораториях в настоящее время возможна в вариантах:

1. ИЛ пользуется полностью автоматизированной системой документооборота с использованием сертифицированной LIMS (система управления лабораторной информацией) – зарубежные системы LIMS, у нас – Qcontrol и др.
2. ИЛ создает подобную систему самостоятельно под свои конкретные условия, включая в нее автоматизированное управление оборудованием, сбором, обработкой и хранением данных и проводит ее валидацию, аттестацию, сертификацию и пр. с привлечением уполномоченных организаций. (Требование 17025). Сама ИЛ не способна «должным образом оценить пригодность» такой системы. В данном случае обеспечение защиты компьютеризированной системы возможно, если коды доступа к ней известны только третьей стороне, например, уполномоченному сервисному центру или подразделению более высокого уровня в организации – специализированному отделу (требуется исключение конфликта интересов).
3. ИЛ использует компьютеризированную систему, включающую полностью автоматизированное оборудование и отдельно обработку результатов, например:

- сбор данных измерений, полученных с использованием программного обеспечения автоматизированного оборудования (исходные данные хранятся в компьютерной системе, защищенной изготовителем оборудования от любого изменения);

- копирование результатов измерения во временный файл в формате, используемом для дальнейшей обработки результатов (Excel), и их передача в центр обработки результатов посредством электронного носителя (флешки, диска) или с использованием локальной компьютерной сети;

- создание файла обработки данных, обработка результатов измерений с использованием «коммерческого готового программного обеспечения» или сертифицированной программы обработки результатов анализа конкретного объекта на регламентированные параметры, получение результата анализа, проведение контрольных процедур;

- создание файла с отчетными данными, утверждение протокола, сканирование оригинала и сохранение скан-копии.

1. ИЛ использует частично компьютеризированную систему, включающую:

- сбор данных измерений, полученных с использованием программного обеспечения автоматизированного оборудования, но не в электронном виде, а в виде распечатки, причем возможности хранения данных в памяти прибора нет;

- сбор данных измерений, полученных оператором при визуальном наблюдении процесса измерения и их регистрация на бумажном носителе (аналогично, если оператор регистрирует данные немедленно после получения на электронный носитель, вводя их вручную);

- ввод данных измерений, зарегистрированных на бумажном носителе, и/или копирование результатов измерения на электронном носителе во временный файл в формате, используемом для дальнейшей обработки результатов, и их передача (через электронный носитель – флешку, диск, по локальной сети) в центр обработки результатов;

- создание файла обработки данных, обработка результатов измерений с использованием «коммерческого готового программного обеспечения», получение результата анализа, проведение контрольных процедур;

- создание файла с отчетными данными, утверждение протокола, сканирование оригинала и сохранение скан-копии.

1. Комбинация 3 и 4 варианта.

**3) Обеспечение аутентичности первичных данных измерений, обработки результатов испытаний и отчетных документов для систем электронного документооборота в ИЛ**

**1 и 2 варианты** – аутентичность всех данных обеспечена разработчиком компьютерной системы документооборота, что подтверждено лицензиями, свидетельствами, аттестацией и т.д., выданными уполномоченными организациями. У пользователя не должно быть никаких проблем с подтверждением требований ГОСТ ИСО/МЭК 17025, т.к. система полностью защищена от любого изменения данных разработчиком на всех этапах испытаний.

**3 и 5 варианты** – аутентичность можно подтвердить только в части тех данных, которые получены, зарегистрированы, обработаны и хранятся в защищенных компьютерных системах, созданных производителями оборудования.

Исключение: в 3 варианте при использовании полностью защищенного ПО оборудования и сертифицированной программы обработки и выдачи результатов. Если в такой программе предусмотрено хранение данных в условиях защищенности, аутентичность обеспечена для всех данных. Специальной защиты для данных в процессе их импорта в обрабатывающую программу в данном случае не требуется, необходимо обеспечить лишь их адекватность (правильность), что не является сложной задачей. Правильность передачи данных подтверждается путем простого сличения.

**4 вариант** – на всех этапах испытания регистрация данных производится вручную.

**Аутентичность данных обеспечивается записями на бумажном носителе** (ведение журналов), причем такой подход считается достаточно надежным, хотя и здесь данные «можно модифицировать, не оставив каких-либо следов». **Важно, чтобы эти журналы были прошиты, страницы пронумерованы и скреплены печатью (на последней странице наклеивается этикетка, в которой указывается: «Прошнуровано (прошито), пронумеровано, количество страниц, подпись вышестоящего лица с расшифровкой подписи».**

Подписи руководителя лаборатории недостаточно, т.к. в данном случае он является заинтересованным лицом. Если в лаборатории руководитель является также и директором, то возможно прикрепить две подписи – руководителя и менеджера по качеству.

**Таким образом, специальное (законодательно регулируемое) программное обеспечение и ведение записей на бумажном носителе (испытанное временем) считаются надлежащим (надежным) средством защиты данных.**

**При ведении документации полностью в электронном виде с использованием обычных текстовых редакторов** (Microsoft Office) с распечаткой данных и их оформлением в «журнал» с определенной периодичностью **аутентичность практически невозможно обеспечить, даже если он будет оформлен как бумажный журнал.**

Рассмотрим набор средств по защите данных, обычно используемый лабораторией, так называемые **пользовательские (внутрилабораторные) средства по защите данных**.

1. **Использование паролей и идентификация пользователей** для доступа к компьютеру при регистрации или обработке данных **позволяет только исключить доступ посторонних лиц (т.е. конфиденциальность)** и частично сотрудников, но не аутентичность данных.
2. **Использование внешних носителей, дублирующих жестких дисков обеспечивает только сохранность данных, их дублирование и возможность восстановления,** но не аутентичность данных**.** В любой момент любой человек, имеющий доступ к дубликатам записей, может их просто заменить, ведь даже диск однократной записи можно заменить на новый (и там будут стоять все правильные атрибуты, включая даты записей). Никакой электронный носитель не прошьешь дыроколом и не подошьешь в папку. Опечатывание в сейфе – а кто опечатывает? (сотрудник лаборатории, имеющий доступ).
3. Даже если после завершения цикла анализа оператор отправляет все данные (и результаты) в центр обработки (выдачи протоколов) и у него на рабочем месте не остается никакой информации, все равно остается круг лиц, имеющих доступ к данным. Этими лицами является руководство лаборатории (заместитель, менеджер по качеству и т.п.). **Никакой формат и никакая форма записи данных** **на персональном компьютере** (пароль, доступ только для чтения, перевод в формат pdf, сохранение скана документа) **не может быть абсолютной гарантией, что их невозможно изменить**.

Проблема именно в том, что в лаборатории всегда будет лицо, имеющее доступ ко всем данным[.](https://rosakkreditatsiya-forum.ru/)

**4) Пути решения проблемы обеспечения аутентичности данных для частично компьютеризированных систем документооборота в ИЛ**

Сейчас трудно найти лабораторию, не использующую ПК для обработки данных и выдачи результатов. Компьютерные ЛИМС эффективны для крупных организаций, средним и малым предприятиям удобнее пользоваться формами регистрации данных, созданным на основе стандартного коммерческого ПО.

В принципе, задача обеспечения аутентичности данных – это создание условий, исключающих возможность их изменения или наличие свидетельств, позволяющих подтвердить уникальность данных (их происхождение).

Не очень приемлемое решение – дублирование всех данных и расчетов с момента выхода данных из защищенной системы на бумажный носитель (ведение журналов).

Возможные приемлемые решения:

1. Вполне логично предположить, что данные можно считать аутентичными, если «жизненный цикл» испытания от момента получения первичных данных до выдачи результатов будет сопровождаться обеспечением аутентичности «надежными средствами» только на самых важных этапах и внутрилабораторными средствами защиты на всех остальных. Например:

**Возможно регистрировать в бумажных журналах факт поступления пробы, первичные данные измерений и только конечные результаты**, которые вносятся в протоколы. Промежуточные расчеты производятся и хранятся в обычных компьютерных системах, распечатываются, подписываются, брошюруются и/или файл обработки данных получает пароль, статус «только для чтения», переводится в формат pdf, копируются на диск однократной записи и т.д.

Примечание 1. Защищенный пользовательскими средствами электронный журнал может состоять из отдельных файлов, формируемых в течение отчетного срока (рабочая смена или неделя, и т.п.). В случае если электронный журнал является одним файлом, куда заносятся данные постоянно (или за длительный период времени), то пользоваться им должен ограниченный круг сотрудников. Наилучший вариант, когда оператор работает с одним рабочим временным файлом, а ответственный сотрудник (лицо, которому известен пароль, код доступа) после проверки вставляет его в электронный журнал, рабочий файл уже не является документом и может быть уничтожен через какое-то время (допустим, месяц).

Примечание 2. Следует иметь в виду, что надлежащая защита данных касается в большей степени данных испытаний. Для документации Системы менеджмента качества, в том числе регистрационных журналов, подтверждающих обеспечение условий проведения испытаний (реактивы, растворы, стандартные образцы, оборудование, нормативные документы, квалификация персонала и т.д.) достаточно обычных пользовательских средств защиты данных.

1. **Все данные по испытанию переносятся на внешний носитель** (диск однократной записи) и в день выдачи результатов анализа (протокола) или в конце недели изымаются из лаборатории, **передаются третьим лицам** или в вышестоящий отдел организации, в который сотрудники лаборатории в принципе не имеют доступ (опять же требуется исключение конфликта интересов)[.](https://rosakkreditatsiya-forum.ru/)
2. В ГОСТ Р 54989-2012 упоминаются два способа, для обычных пользователей мало известных, требующих знаний программистов, а именно:

**Контрольные суммы машинного кода CRC и применение односторонних хэш-функций**. Именно такие способы используют различные специальные компьютерные программы.

Возможно, это решение проблемы (?)

**5) Выводы**

Из вышеизложенного, доступной информации из форумов, опыта общения с экспертами, а также здравого смысла, можно сделать следующие выводы:

Поскольку абсолютную аутентичность данных при частично компьютеризированном документообороте в лаборатории в реальности не обеспечить, то в некоторых лабораториях внедрен следующий подход: **Регистрация входящих данных о пробе на бумажный носитель (журнал регистрации проб), первичных данных измерений (журнал результатов измерений), полученных при визуальном считывании, и регистрация выходных данных – результатов анализа, которые заносят в протокол (журнал выдачи результатов).**

Все записи, относящиеся к промежуточным стадиям процедуры анализа, должны иметь защиту от несанкционированного доступа посторонних лиц и защиту от внесения изменений сотрудниками лаборатории после окончания регистрации и обработки данных. Здесь как раз и применяется весь спектр пользовательских способов защиты.

Требуется ли для обычной Испытательной лаборатории среднего и малого предприятия специальные программы по защите данных, вплоть до криптографических?

Предполагается, что только для законодательно регулируемых сфер деятельности.

В обычной производственной деятельности, скорее всего – нет. **Главный лейтмотив международного стандарта по менеджменту качества ИСО 9001 – предпринятые действия должны быть всегда соизмеримы существующим рискам**.