**ИСПЫТАТЕЛЬНЫЙ ЦЕНТР**

УТВЕРЖДАЮ:

Руководитель ИЦ

\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_202\_\_\_ г*.*

ИНСТРУКЦИЯ

**ВАЛИДАЦИЯ КОМПЬЮТЕРИЗИРОВАННЫХ СИСТЕМ**

**РИ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## Содержание

[1. Область применения 3](#__RefHeading___Toc5872_2092707262)

[2. Определения 3](#__RefHeading___Toc5874_2092707262)

[3. Аппаратная часть 4](#__RefHeading___Toc5876_2092707262)

[4. Общие требования к программному обеспечению 4](#__RefHeading___Toc5878_2092707262)

[5. Валидация программного обеспечения для расчетов 7](#__RefHeading___Toc5880_2092707262)

[7. Валидация компьютеров как части аналитического оборудования 10](#__RefHeading___Toc5882_2092707262)

[8. Валидация баз данных, лабораторных информационных систем (ЛИС) и электронных лабораторных журналов (ЭЛЖ) 11](#__RefHeading___Toc5884_2092707262)

[8.1. Валидация баз данных 11](#__RefHeading___Toc5886_2092707262)

[8.2. Валидация ЛИМС/ЭЛЖ 15](#__RefHeading___Toc5888_2092707262)

[8.3. Валидация имеющегося в наличии программного обеспечения 19](#__RefHeading___Toc5890_2092707262)

[9. Валидация компьютерных система в составе аналитического (испытательного оборудования) 20](#__RefHeading___Toc5892_2092707262)

[10. Планирование и документирование валидации ПО и компьютерных систем 23](#__RefHeading___Toc5894_2092707262)

[11. Эксплуатация ПО 29](#__RefHeading___Toc5896_2092707262)

[Приложение 1 32](#__RefHeading___Toc5898_2092707262)

[Приложение 2 33](#__RefHeading___Toc5900_2092707262)

[Приложение 3 37](#__RefHeading___Toc5902_2092707262)

[Приложение 4 41](#__RefHeading___Toc5904_2092707262)

[Приложение 5 42](#__RefHeading___Toc5906_2092707262)

[Приложение 6 43](#__RefHeading___Toc5908_2092707262)

[Приложение 7 45](#__RefHeading___Toc5910_2092707262)

[Приложение 8 46](#__RefHeading___Toc5912_2092707262)

[Приложение 9 47](#__RefHeading___Toc5914_2092707262)

## **1. Область применения**

Эта инструкция определяет основные принципы валидации компьютеризированных систем, используемых в лабораториях с уклоном на качество результатов. Целью этой валидации является обеспечение уверенности в результатах, полученных от каждой компьютеризированной системы. Валидированная система обеспечивает точные результаты и снижает риск выхода системы из строя.

Этот документ охватывает программное обеспечение как внутренней разработки, так и коммерческое, применяемое для расчетов, системы управления базами данных (СУБД), Лабораторные информационные системы (ЛИМС/ЛИС), электронные лабораторные журналы (ЭЛЖ) и компьютеры, в рамках аналитического оборудования. Эта инструкция описывает общие принципы валидации компьютеризированных систем в соответствии с ISO/IEC 17025. Инструкция выдвигает общие требования, а также перечисляет минимально необходимые элементы для проверки различных типов программного обеспечения. Из-за большого разнообразия программного обеспечения, не представляется возможным изложить в одном документе все конкретные применяемые элементы проверки (см. далее).

Эта инструкция предназначено для использования лабораториями, работающих по системе менеджмента на основе стандарта ГОСТ ISO/IEC 17025-2019, которые используют автоматизированные системы для части или совокупности процессов, связанных с контролем качества.

Для того, чтобы упростить применение этой инструкции, настоящий документ содержит только общие указания и требования для различных типов автоматизированных систем. Также базовый документ дополняется, системозависимыми приложениями, содержащими дополнительные требования и/или практические примеры валидации документации, которые должны использоваться в сочетании с общими рекомендациями, изложенными в основном документе.

Список приложений, включенных в этот документ будет обновляться по мере выпуска новых приложений.

Этот документ следует рассматривать как руководство для планирования, выполнения и документирования валидации компьютеризированных систем.

## 2. Определения

**Компьютерная система** — аппаратные компьютерные компоненты в сочетании с набором программного обеспечения, которые вместе предназначены для выполнения определенной функции или группы функций.

**Компьютеризированная система** — компьютерная система, плюс контролируемая функция, которую она выполняет. Включает в себя оборудование, программное обеспечение, периферийные устройства, персонал и документацию, например, руководства и стандартные операционные процедуры (СОП).

**Коммерческое (готовое, настраиваемое) программное обеспечение** — настраиваемые программы, которые могут быть настроены для конкретных задач пользователя, путем «заполнение пробелов (пустот)», без изменения основной программы.

**Программное обеспечение собственной разработки** — специальная система, разработанная пользователем (или по контракту компанией), с целью удовлетворения определенного набора требований пользователя.

**Электронный лабораторный журнал (ЭЛЖ)** — программное обеспечение (программа), предназначенное для замены бумажных лабораторных журналов.

**Лабораторная информационно система (ЛИС/ЛИМС)** — автоматизированная лабораторная система, которая собирает и обрабатывает (управляет) данные (ми).

## 3. Аппаратная часть

Используемое аппаратное обеспечение, должно отвечает техническим требованиям настолько, чтобы поставленная работа была выполнена. Такие требования включают, например, минимальные системные требования, указанные заводом-изготовителем оборудования. Эти требования должны быть заранее определены в соответствии с предполагаемым использованием.

Аппаратные компоненты должны быть установлены квалифицированным персоналом (например, сотрудниками отдела Информационных Технологий (ИТ), техническим сотрудником производителя оборудования или другим квалифицированным персоналом), а также должна быть проверена их функциональность в сравнении с установленными требованиями.

Компьютеризированные системы, которые являются частью аналитического оборудования должны иметь однозначную маркировку.

Для компьютеризированных систем, которые являются компонентами аналитического оборудования, записи должны вестись от конфигурации оборудования, монтажа и внесения изменений. Эти записи могут быть внесены в журнал протоколирования аналитического оборудования.

## 4. Общие требования к программному обеспечению

Реестр

Должен быть доступен реестр или список всех компьютеризированных систем.

Следующая минимальная информация должна быть включена в реестр компьютеризированных систем:

* уникальный идентификатор
* применение
* состояние валидации или валидационный статус
* физическое или место хранения (диск и пути к файлам) местонахождение программного обеспечения и сопутствующей документации
* ответственное или контактное лицо

В случае локальной установки (рабочая станция), каждая копия программного обеспечения должна иметь свой собственный уникальный идентификатор.

В случае программного обеспечения, связанного с научным оборудованием (например, ВЭЖХ) его идентификатор (например, номер лицензии или серийный номер и номер версии) должен быть по возможности независимыми от идентификатора оборудования.

Валидация программного обеспечения

Перед обычным использованием, программное обеспечение должно быть валидировано.

Валидация заключается в подтверждении путем проверки и предоставлении объективных доказательств того, что спецификации программного обеспечения соответствуют потребностям пользователей и предполагаемому использованию, а также, что специальные требования реализуемые с помощью программного обеспечения могут последовательно выполняться.

Контроль за изменениями

В случае внесения изменений в программное обеспечение, должна быть проведена валидация состояния системы. Если необходим перепроверяющий анализ, то он должен быть проведен не только для проверки отдельных изменений, но также и для определения масштаба и последствия этого изменения для всей компьютеризированной системы.

Таким же образом, изменения в аппаратной среде могут повлиять на работающее программное обеспечение. В этом случае может потребоваться ревалидация.

В обоих случаях объем ревалидации, будет зависеть от характера изменений.

Характер изменений должен быть задокументирован.

Автоматические обновления, в идеале, должны находиться под контролем ИТ департамента или системного администратора и устанавливаться в предварительно заданные даты, чтобы минимизировать как разрушение так и неожиданное поведение системы. После установки обновлений, должна быть проведена валидация, степень которой будет зависеть от степени обновления(й).

Каждое обновление должно быть задокументировано.

Примечание: это не обязательно относится к сервисным обновлениям коммерческого офисного программного обеспечения.

Верификация программного обеспечения

Коммерческое программное обеспечение должно быть проверено во время установки.

Что касается программного обеспечения собственной разработки, то оно должно проверяться не только во время установки, но и в целом регулярно, чтобы избежать любых ошибок и гарантировать хорошие результаты. Регулярность верификации зависит от безопасности программного обеспечения, частоты использования и возможных последствий в случае неудачи.

Защита программного обеспечения

Программное обеспечение должно быть защищено от любого вторжения, которое может вызвать искажение научных результатов. Одним из способов защиты программного обеспечения или компьютеров/систем является доступ с помощью пароля. Он также должен быть защищен от любых внешних вмешательств, которые могут изменить данные, и повлиять на окончательные результаты.

Резервное копирование

Прослеживаемость данных должна быть обеспечена от исходных данных к результатам. Если все или часть отслеживаемых параметров, которые важны для качества результатов, доступны только в электронном виде, то должен быть реализован процесс резервного копирования для обеспечения восстановления системы после любых неполадок, которые подвергают опасности её целостность. Частота резервного копирования зависит от критичности данных, объем хранимых данных и частоты их создания.

Лаборатории должны иметь стратегию и установленные процедуры для обеспечения целостности резервных копий (безопасное место хранения, достаточную удаленность от основного места хранения, и т.д.) — эти мероприятия могут быть частью более общего «плана аварийного восстановления».

В наличии также должны присутствовать процедуры по регулярному тестированию резервных данных (тест восстановления), проверке надлежащей целостности и точности данных.

Архив заменены версий программного обеспечения

Замененные версии программного обеспечения следует архивировать (если требуется доступ к данным за прошлые года) на срок как минимум 5 лет, в электронном формате, который можно легко восстановить и прочитать.

*Примечание: данное требование не распространяется на коммерческие готовое к использованию офисное программное обеспечение (включая сервисные обновления), программное обеспечение, которое архивировано квалифицированным субподрядчиком или когда данные за предыдущие периоды (исходные данные и результаты) документированы в бумажном формате.*

Определение версии программного обеспечения

Версия и название программы должны отображаться пользователю на соответствующей стадии эксплуатации программного обеспечения (например, на экране при открытии приложения), также они должны отражаться в любых отчетах, генерируемых данным программным обеспечением.

Для лабораторного программного обеспечения на компьютерах в составе аналитического оборудования, обновление программного обеспечения, включая номер версии должны быть отражены в журнале оборудования.

Обзор компьютеризированных систем

Для компьютеризированных систем должны регулярно проводится действия по управлению рисками и/или аудит.

Подготовка операторов программного обеспечения

Должна быть обеспечена корректная работа программного обеспечения. Это может быть выполнено либо путем соответствующей и документированной подготовки или путем изложения детальной информации в соответствующих СОП.

## 5. Валидация программного обеспечения для расчетов

Для расчетов и анализа данных может использоваться коммерческое программное обеспечение или собственной разработки.

Запрашиваемая документация/информация, применительна к обеим типам ПО и указана в Таблице I.

а) Коммерческое программное обеспечение

Если доступны несколько образцов коммерческого программного обеспечения, лаборатория может выбрать тот, который лучше соответствует назначению.

В соответствии с стандартом ГОСТ ISO/IEC 17025-2019 коммерческое готовое к использованию программное обеспечение (например, текстовые процессоры, базы данных и статистические программы), в установленных пределах его общего использования, может считаться достаточной степени валидированным. Тем не менее, конфигурации/изменения лабораторного ПО должны валидироваться.

Сократить процедуру валидации (этих конфигураций/модификаций) допускается в случае, если в документации, поставляемой с готовым к использованию коммерческим ПО были пересмотрены, согласованы и выполнены все требования пользователей.

б) Программное обеспечение собственной разработки

Если используется ПО собственной разработки, то оно должно находится под наблюдением основного пользователя (прим. имеется ввиду того, которые его разработал и поддерживает в актуальном состоянии), должно быть валидировано, проверено и защищено, подробную информацию о валидации см. в п. 8 и 9.

Основные требования

— Что касается электронных таблиц (например, Excel®), в целях безопасности, все ячейки, содержащие расчеты должны быть заблокированы таким образом, чтобы формулы не были случайно перезаписаны. Свободный доступ должен быть предоставлен только к ячейкам в которые заносятся исходные данные. Формулы должны быть защищены от случайного ввода неподходящего типа данных (например, текста в числовое поле).

— Каждый алгоритм расчета должен быть проверен на другом программного обеспечении (версия программного обеспечения использованного для расчетов должна быть отражена в записи) или с помощью ручного пересчета, или с помощью калькулятора и задокументирован или необходимо сравнивать результаты расчетов с известными литературными данными.

— Для верификации ПО должен быть использован известный набор данных для которого также известны идентифицированные и проверенные результаты.

Валидация расчетных систем должна проводится независимо от их происхождения. Для валидации пользователь подготавливает набор требований и данных с указанием:

* Вид ПО, версия, идентификатор, описание расчетной формы
* Ссылки на используемую методику расчета
* Формулы, используемые в расчете
* Значения, используемые в валидационном отчете;
* Методы защиты данных от изменения (формул от искажения)
* Местонахождение проверенной версии ПО.

Дополнительно пользователь может подготовить скриншоты (снимки) валидируемого ПО, записи подтверждающие проверку расчетов на альтернативном ПО.

Для расчетов используются позитивные и негативные тесты на рабочих данных, так и бессмысленные наборы данных, в том числе за пределами спецификации (аттестации) методов расчета. Также могут использоваться недостающие данные, для проверки расчетов пустых и нулевых значений.

Позитивные тесты

В ходе позитивных тестов подтверждают, что все формулы дают правильные результаты для различных наборов входных данных. Для проверки рекомендуется использовать как минимум два набора данных, для которых заведомо известно, что один из них дает правильные результаты, а второй дает неправильные. Также включите в проверку наборы пограничных данных для подтверждения прецизионности ваших формул. В завершение, перепроверьте результаты электронной таблицы с помощью расчетов вручную. Рекомендуется использовать как рабочие данные, так и бессмысленные наборы данных.

Негативные тесты

В ходе негативных тестов используют неправильные входные данные, для которых известно, что они дают неправильные результаты. Эти тесты подтверждают надежность электронной таблицы, то есть то, что её активный документ выдерживает ввод неправильных данных без краха приложения, выдачи неправильных результатов или даже обхода безопасности.

Примеры негативных тестов включают:

* Оставление полей ввода пустыми для удостоверения в том, что система проверки на незаполненные обязательные поля работает корректно.
* Ввод в числовое поле буквенных или специальных символов.
* Ввод в целочисленное поле десятичной дроби.
* Ввод отрицательных чисел в поле положительных чисел.
* Ввод бессмыслицы.
* Ввод в поле большего количества символов, чем разрешено для этого поля.
* Ввод даты, выходящей за пределы верхней и нижней границы дат.

В результате оформляется протокол валидации расчетов в ПО по форме указанной в приложении 1.

При необходимости устанавливается срок верификации расчетов, когда пользователь проверяет ПО с использование того же набора данных и оформления Протокола верификации (по форме указанной в приложении 1 с добавлением сведений о протоколе первичной валидации).

При внесении изменений в расчетные формы проводят ревалидацию ПО. Все изменения должны быть задокументированы.

Таблица I: Документация программного обеспечения

|  |  |  |
| --- | --- | --- |
| **Информация / документации, которая должна быть доступна** | **Коммерческое ПО** | **ПО собственной разработки** |
| Название, версия и уникальный идентификатор ПО | X | X |
| Оригинальные файлы (CD-ROM …) или место хранения для установки ПО и ПО для управления компьютерным окружением | X | X |
| Дата ввода ПО в эксплуатацию | X | X |
| Текущее физическое местоположение, если необходимо | X | X |
| Ответственное лицо, отвечающее за программное обеспечение | X | X |
| Название Производителя, номер лицензии и серийный номер или другой уникальный идентификатор | X |  |
| Условия, при которых программа запускается в работу, если это потребуется (аппаратное обеспечение, операционная система, …) | X | X |
| Сертификат валидации ПО от производителя, если таковой имеется | X |  |
| Инструкции производителя, если таковые имеются, или ссылки на их местонахождение | X |  |
| Документация по валидации конфигурации / модификации, выполненные пользователем, которые могут повлиять на результаты (см. приложения) | X |  |
| Ф. И. О. лица, разработавшего и валидировавшего ПО, а также дата валидации |  | X |
| Исходный код, если доступен |  | X |
| Правила эксплуатации, при необходимости |  | X |
| Документация по регулярной верификации ПО | X | X |
| Документация по валидации ПО (см. Приложения) | X | X |
| Порядок действий при возникновении сбоев, поддержание рабочего процесса, обновление версий и, при необходимости, управления конфигурациями | X | X |

## 7. Валидация компьютеров как части аналитического оборудования

В некоторых методах испытаний (например, ВЭЖХ, подсчет частиц), используется аналитическое оборудование, которое управляется компьютеризированной системой. При этом исходные данные в целом, также оцениваются непосредственно через компьютер. Таким образом, качество таких результатов, во многом зависит от правильного использования программного обеспечения и функциональности компьютеризированной системы. Для более подробной информации о валидации см. п. 9

В рамках квалификации оборудования, компьютеризированная система, а также программное обеспечение, связанное с ней, должны быть проверены с точки зрения надежности, точности и воспроизводимости (этого возможно может быть достаточно, чтобы квалифицировать аналитическое оборудование с программным обеспечением в целом).

Ревалидация требуется в том случае, если изменения в компьютеризированной системе (аппаратном или программном обеспечении) могут повлиять на качество результатов испытаний.

## 8. Валидация баз данных, лабораторных информационных систем (ЛИС) и электронных лабораторных журналов (ЭЛЖ)

## 8.1. Валидация баз данных

Базы данных, используемые для хранения и поиска результатов испытаний, подготовки протоколов испытаний, которые были разработаны собственными силами или поставлены в лабораторию на коммерческой основе считаются достаточно валидированными.

Тем не менее, следующая минимальная документация/информации должна быть в актуальном состоянии, в соответствующем файле каждой базы данных:

* Схематическое представление базы данных.
* Должны отслеживаться изменения форм, запросов, макросов, типов полей или свойств, которые могут влиять на качество результатов.
* Каждый пользователь должен иметь персональный код доступа.
* Должны быть определены права пользователей.
* Должны записываться операционные правила.
* Любые модификации по улучшению или ухудшению должны документироваться.

Уровень I. Выбор программного обеспечения и компьютерного оборудования

Это первый шаг валидации. Спецификация требований пользователей или техническое задание (ТЗ) описывает функциональные, технические и организационные требования к системе определяемой заказчиком. Реализации и верификация проводятся в соответствии с этими ТЗ.

(1) Описание используемого программного обеспечения, в том числе версии (например Excel, Access, Oracle)

(2) Требования к компонентам оборудования и операционной системе

(3) Описание функций

(4) Описание атрибутов данных

(5) Терминология (например, важно для унифицированной записи масок ввода/полей)

(6) Проектирование базы данных, включая маски и поля, а также карты взаимосвязи данных

(7) Спецификации макросов, формул и команд управления

(8) Спецификации вводимых данных (например, формат, число десятичных знаков, единицы измерения)

(9) Спецификация обязательных полей для данных

(10) Спецификации масок защиты, рабочих листов или всего приложения

(11) Планирование переноса данных, если применяется

(12) Спецификации интерфейсов к другими компонентами системы, если применяется

В случае простой базы данных, достаточно схемы управляемого потока данных, как дизайна базы данных. Спецификации (ТЗ), должны быть разрешены ответственным лицом. Возможны изменения по требованиям. Изменения должны прослеживаться, а ТЗ в этом случае получает новый номер версии. Новые или измененные требования должны быть донесенны до всех заинтересованных лиц.

Уровень II. Установка и выпуск для использования

Правильная установка системы в ИТ-среде с определенным аппаратным и программным обеспечением, документируется и тестируется. В большинстве случаев, БД, ЛИМС или ЭЛЖ встраиваются в компьютерную сеть с интерфейсами к другому программному и аппаратному обеспечению. Должна быть обеспечена правильная интеграция системы, а также функционирование всех компонентов.

Установка

(1) Проверка необходимых для системы ресурсов (например, производительность процессора, количество свободного места на жестком диске, доступ для установки)

(2) Документация к компонентам системы (как минимум описание компонента и версии соответствующих компонентов с датой внедрения)

(3) Список пользователей или групп пользователей, имеющих доступ к приложению, в том числе тип доступа

(4) Тест интеграции и/или подключения (например, хранение набора известных данных в базе данных и обработка данных, если запрограммирован процесс расчета или другой процесс, восстановление и печать данных и сравнение с критериями приемлемости)

Частота установки поддерживается поставщиком и внутренним ИТ-отделом.

Выпуск для использования

(1) Анализ проекта

(2) Тесты функций (например, каждая функция базы данных проверяется на наборе данных)

(3) Отрицательные испытания или испытания с предельной нагрузкой (например, ввод значений вне указанного диапазона)

(4) Тестирование предупреждающих сообщений, если применимо (например, отображение результата за пределами спецификации)

(5) Несанкционированный ввод данных и доступ к приложению

(6) Тесты неверного ввода (например, ввод данных в неправильном формате данных)

(7) Тест системы резервного копирования и восстановления

(8) Верификация переноса данных, если применяется

(9) Соответствие требованиям защиты информации, если применяется

(10) Тест «черный ящик», как приемо-сдаточное тестирование системы в целом

На этом участке должно быть проверено соответствие ТЗ.

Число наборов данных, используемых для функциональных испытаний, зависит от оцененного класса риска. Должны применяться, как минимум, два значения в пределах нормы.

В качестве теста на предельную нагрузку или отрицательного теста, должно использоваться, как минимум, одно значение ниже и одно значение выше предела. Такой же алгоритм тестирования может быть использован для проверки функции предупреждающих сообщений.

В случае базы данных с большим количеством функций, возможно уменьшение размера теста до ключевых функций. Это решение основывается на оценке риска и должно документально прослеживаться. Также возможно выполнять тесты «черного ящика» для наиболее важных вариантов использования базы данных вместо тестирования отдельных функций.

Чтобы показать надежность базы данных, выполняется несанкционированный и неправильный ввод данных.

Верификация переноса данных следует с шести записей вплоть до 100% переносимых данных. Случайная выборка зависит от оцененного класса риска. Данные целевой системы, сравниваются с данными исходной системы. Для таких видов верификации доступны автоматизированные инструменты.

Уровень III. Периодические и целенаправленные проверки функциональности программного обеспечения

Периодические проверки (тест «черного ящика»), особенно после серьезных изменений и с регулярной периодичностью, выполняются для обеспечения корректной работы всей системы в течение срока эксплуатации.

Документация

В дополнение к списку программной документации, в соответствии с базовым документом валидации компьютеризированных систем, некоторые специальные аспекты должны быть в описании.

(1) Системное описание базы данных (например, диаграмма системы, программный процесс, взаимосвязи ячеек и таблиц, макросы, формулы)

(2) Скриншоты соответствующих рабочих листов и масок

(3) Спецификация требований пользователя, как минимум последняя актуальная версия ТЗ

(4) Отчеты квалификации установки, включая конфигурацию

(5) Описания теста, записи и результаты верификации

(6) Отчет по валидации, если применяется

(7) Уникальный идентификатор версии базы данных

(8) Обучающие планы и записи, если применяется

(9) Руководство пользователя, если применяется

(10) Сопроводительная документация, если применяется

Документация должна позволять прослеживать валидацию, а также техническое обслуживание и разработку базы данных в любой момент её жизненного цикла, третьей стороной. Каждое изменение в документах должно быть прослеживаемым.

Администрирование

Эта часть не является типичным этапом процесса валидации, но она содержит информацию, которая имеет отношение к спецификации и валидации системы.

База данных является валидной в течение всего времени использования, если гарантируется поддержание её работоспособности.

(1) Управление конфигурацией (конфигурация компьютерной системы, которая содержит базу данных, должна прослеживаться в любой момент времени, включая дату интеграции новых компонентов или версий)

(2) Управление изменениями (все изменения в дизайне базы данных должны прослеживаться, а для серьезных изменений требуется предварительное разрешение ответственного лица)

(3) Управление патчами и обновлениями операционной системы (как минимум, документируются осуществлявшиеся патчи и обновления, правила применения патчей/обновлений, например, в ночное время или на выходных, тест «черного ящика» после установки патча/обновления в случае необходимости)

(4) Управление постоянством и сбоями (сбор списка отклонений сбоев, например, корректирующее действие и предупреждающее действие/КДПД(CAPA))

(5) Организация службы технического сопровождения, если применяется

(6) Безопасное копирование приложения

(7) Защита данных (Логин, пароль, права доступа)

(8) Стратегия резервного копирования (например, промежуточное, инкрементное или полное резервное копирование, интервал времени)

(9) Понятие аварийного восстановления, если применяется

(10) Концепция обучения, если применяется

В случае простой базы данных, требования по её администрированию сокращаются. Вышеприведенный список справедлив в основном для сложных баз данных.

Должна быть прописана ответственность за управление конфигурацией между внутренним ИТ-подразделением и лабораторией. Также это важно для управления патчами и обновлениями, а также для резервного копирования.

## **8.2. Валидация ЛИМС/ЭЛЖ**

Для коммерческих Лабораторных Информационных Систем (ЛИМС) и Электронных Лабораторных Журналов (ЭЛЖ), система валидации должна свидетельствовать, что программное обеспечение полностью и надлежащим образом протестировано. Для более подробной информации о валидации см. в Приложении 2.

Валидация любой модификации, конфигурации или расчетов, которые могут оказать влияние на результаты, находится в зоне ответственности пользователя (см. пункт 5.a и в таблице 1 для коммерческого программного обеспечения).

Масштабируемый подход на основании степени валидации

Уровень риска влияет на степень валидации. В этом случае требуется оценка рисков. Оценка риска включает анализ возможного влияния компьютеризированной системы на качество и целостность данных.

Уровень и степень валидации в дополнение к риску, зависит от категории программного обеспечения.

Компьютеризированная система может чаще всего рассматриваться следующим образом:

Инфраструктурное программное обеспечение, например, операционные системы или менеджер баз данных

Не настраиваемое программное обеспечение (части), например приложение-прошивка

Настраиваемое программное обеспечение (части), например, интерфейсы к устройствам или другое программное обеспечение

Специализированное программное обеспечение (части), например, Excel с макросами, настроенные по своему усмотрению диалоговые окна

Инфраструктурное программное обеспечение требует документирования версий программного обеспечения и конфигурации, а также выполнения квалификации установки. Валидация специализированного программного обеспечения содержит описание спецификаций требований пользователей, анализ кода и дизайна, документацию версий и конфигурации, квалификацию установки, тесты функций на основе рисков и предопределенное управление данными.

При таком подходе нет необходимости осуществлять подобные действия для всей системы. Валидация будет описана индивидуально для каждой части системы.

Использование работы поставщика

Валидация документов и результаты испытаний, проведенные поставщиком программного обеспечения, могут быть перенесены в собственную валидацию. Эта работа и испытания не должны повторяться заказчиком. Поставщик должен быть предварительно квалифицирован (например с помощью анкетирования или аудита).

План валидации

Для обеспечения проведения корректной валидации необходим план валидации. План валидации описывает все действия, такие как анализ спецификаций, анализ схемы разработки (дизайна), алгоритм тестирования, верификаци переносимых данных, анализ валидации документов и приемо-сдаточных испытаний системы в целом.

План содержит дату, данные ответственного лица и критерии приемки для каждого анализа или теста, или как минимум ссылки на эти тесты.

План валидации должен быть разрешен ответственным лицом перед началом валидации.

Контрольные примеры и описания могут быть описаны позже, если используется итерационный процесс. Пример плана валидации приведен в приложении 3.

Фоновым компонентом ЛИМС или ЭЛЖ является работающая база данных. Все требования, которые перечислены в главе «Валидация баз данных», справедливы и для ЛИМС или ЭЛЖ. Аспекты, которые отмечены как «если применяется» в предыдущей главе, в особенности актуальны для ЛИМС.

Специальные указания и дополнительные требования описаны в следующих разделах.

Команде по валидации рекомендуется использовать положения ГОСТ Р 54360-2011 Лабораторные информационные менеджмент-системы (ЛИМС). Стандартное руководство по валидации ЛИМС; ГОСТ Р 53798-2010 Стандартное руководство по лабораторным информационным менеджмент-системам (ЛИМС); ГОСТ 33044-2014 Принципы надлежащей лабораторной практики.

Для валидации создается комиссия (команда) валидации. Типичная комиссия состоит из представителей лаборатории, групп специалистов от организаций по системам управления информацией (ИТ отдела) и подразделений по обеспечению качества. В случае валидации ПО собственной разработки рекомендуется включать в комиссию разработчиков и администраторов ПО. Комиссия по валидации должна начать работать с момента формирования спецификаций требований пользователей и выбора поставщика ЛИМС/ЭЛЖ.

При формировании спецификации должны учитываться требования ГОСТ Р 54360-2011 Лабораторные информационные менеджмент-системы (ЛИМС). Стандартное руководство по валидации ЛИМС; ГОСТ Р 53798-2010 Стандартное руководство по лабораторным информационным менеджмент-системам (ЛИМС); ГОСТ 33044-2014 Принципы надлежащей лабораторной практики; ГОСТ ISO/IEC 17025-2019 Общие требования к компетентности испытательных и калибровочных лабораторий и другие нормативные документы предъявляющие требования к лабораториям и лабораторным информационным системам.

Уровень I. Выбор программного обеспечения и компьютерного оборудования

Спецификация требований пользователей (техническое задание - ТЗ) должна содержать все соответствующие функциональные, технические и организационные спецификации. Она должна охватывать также аспекты информационной безопасности и защиты данных.

Каждое требование должно быть описано в ТЗ отдельной строкой. Каждая строка должна быть обозначена уникальным номером. Этот номер позволяет обращаться к требованию в процессе разработки, а также в процессе валидации.

В случае коммерческого ПО необходим провести оценку и аудит продавца ЛИМС. Оценка продавца должна происходить в течение фазы "оценки и выбора" жизненного цикла ЛИМС и перед окончательным выбором продавца. Если организация уже создала команду по аудиту продавца, эта группа должна рассмотреть требования к функциональностям системы вместе с командой по валидации ЛИМС. Как правило, ответственным за долгосрочное взаимодействие с продавцом должен быть кто-то из команды по аудиту. Обычно это лицо является владельцем системы или приложения.

Первичная цель аудита состоит в том, чтобы гарантировать, что программное обеспечение и процедуры управления продавца соответствуют общепринятым методам, то есть тем, которые поддерживают прослеживаемость вплоть до контрольной точки и которые придерживаются этих методов.

В дополнение к этим задачам организация, проводящая аудит, должна оценить финансовое состояние и стабильность продавца. Следует отметить, что даже если организация продавца ЛИМС зарегистрирована в соответствии с национальными или международными требованиями, например ГОСТ Р ИСО 9001, продавец не освобождается от проведения аудита заказчиками. По-прежнему закупочная организация ответственна за проведение аудита предполагаемого продавца ЛИМС. Основные детали процедуры аудита продавца приводятся в ГОСТ Р 54360-2011.

Уровень II. Установка и выпуск для использования

Лаборатория должна валидировать используемую им ЛИМС, независимо от любых результатов аудита продавца,в той среде функционирования, в которой будет находиться ЛИМС. Тот факт, что продавец валидировал процесс разработки ЛИМС сам или с привлечением других организаций, имеет незначительное отношение к валидации приложения ЛИМС, находящегося в организации. Тот факт, что программное обеспечение продавца ЛИМС было валидировано одним из других заказчиков продавца, не устраняет необходимость для организации валидировать внедрение их приложения.

Следует конфигурировать ЛИМС для регулярных операций, а затем изолировать ее от обычного обслуживания на то время, когда проводится испытание

Должны быть доступны подробные процедуры установки. Установка должна выполняться только хорошо обученным персоналом.

Контрольные списки с предопределенными шагами установки и критериями приемлемости обеспечивают правильную установку системы и прослеживаемость квалификации установки.

Важно, принять во внимание, следующие аспекты процесса валидации:

(1) ИТ сеть (проверка требуемой спецификации системы и технических данных)

(2) Клиенты (должна быть известна конфигурация клиентов)

(3) ЛИМС или ЭЛЖ-сервер (см. пункт ИТ сеть)

(4) Периферийные компоненты и интерфейсы (функция каждого компонента и интерфейса должна быть проверена)

(5) Исходный код программного обеспечения (исходный код, правила кодирования и средства кодирования должны быть известны, а доступ к ним гарантирован)

(6) Данные (целостность данных должна быть показана путем сравнения исходных данных с переобработанными данными, а также использование ограничения доступа и процесса аудита)

(7) Руководства и процедуры (должны быть доступны все соответствующие документы, такие как: процедура установки, описание программного обеспечения, процедуры валидации, обучающие руководства и руководства пользователя, руководство по обслуживанию, процедура резервного копирования и восстановления данных, порядок управления изменениями и документация по разработке)

(8) Поставщик (поставщик должен быть квалифицирован)

(9) Персонал (сотрудники должны быть обучены и квалифицированы, должны быть в наличии стратегия и план обучения конечных пользователей)

Обработка ошибок и критерии приемки должны быть определены и описаны в валидационном протоколе, прослежены в процессе испытания и отражены в отчете о результатах. Определение должно включать критерии, которые используются для того, чтобы оценить серьезность ошибок.

Критические ошибки, такие как сбои системы или фатальные ошибки, выделенные в течение валидационного испытания, должны быть немедленно подвергнуты коррекции или ремонту, перед тем как будет проведено дополнительное испытание. Часто корректировка таких ошибок требует, чтобы большинство или все валидационные испытания были проведены вновь. Имеются такие ошибки, для которых не существует специальных приемов для исправления. Эти ошибки серьезно угрожают целостности данных ЛИМС.

В процессе валидационных испытаний должны быть собраны некритические ошибки. Когда испытание закончено, комиссия может принять решение о том, что эти ошибки не подвергают опасности целостность информации. Имеются ошибки, которые могут привести к тому, что, возможно, системой ЛИМС будут приняты недопустимые результаты. Для таких ошибок могут быть использованы специальные приемы. Классификация ошибок по их влиянию приведена ниже:

0 - типографские ошибки и другие ошибки, не относящиеся к компьютерной системе.

1 - незначительные ошибки, такие как использование прописных и строчных букв на полях, не предназначенных для них.

2 - допустимые ошибки, о которых необходимо сообщить продавцу.

3 - значительные ошибки, о которых необходимо немедленно сообщить продавцу и руководителю подразделения по обеспечению качества. Все работы по валидации должны быть приостановлены, пока уполномоченные специалисты по качеству обсуждают проблему.

4 - катастрофические ошибки, такие как реляционные ошибки в базе данных. О них сообщают таким же образом, как для сорта 3, но работа по валидации должна быть прервана. Специалисты по обеспечению качества могут, однако, принять решение о том, что работа по валидации будет продолжена после всестороннего обсуждения.

Уровень III. Периодические и целенаправленные проверки функциональности программного обеспечения

Периодические проверки (тест «черного ящика») основных функций, по одному контрольному примеру на каждую.

## **8.3. Валидация имеющегося в наличии программного обеспечения**

Предыдущие требования применимы для новых баз данных и ЛИМС/ЭЛЖ.

Для ретроспективной валидации имеющегося в наличии программного обеспечения, в частности, должны быть рассмотрены следующие пункты.

(1) Выполнение оценки рисков

(2) Инвентаризация всех имеющихся документов (например, описания системы, представления, ТЗ)

(3) Верификация правильности установки (например, требования к операционной системе, компьютерной системе)

(4) Создание отчета об опыте работы (резюме опыта работы с программным обеспечением: Как долго это программное обеспечение работает? Какие есть неисправности? Имеются трудности в использовании? И есть ли не задокументированные функции?)

(5) Добавление недостающих документов (как минимум функциональное описание, в виде обзора или базовых спецификаций, рабочих инструкций)

(6) Комплексный тест (позитивный тест - типичное применение с сравнением результата с ожидаемым значением, негативный тест - не типичное поведение с рассмотрением возникающих ошибок)

(7) Формальный выпуск для использования — заключение о пригодности.

Изменения в ПО, а также проведенные валидации должны быть отражены в документации.

## 9. Валидация компьютерных система в составе аналитического (испытательного оборудования)

При разработке аналитических (испытательных) методик, аппаратных комплексов — лаборатория должна обеспечить валидацию этих методик и комплексов, в том числе используемые при их установке и функционировании компьютерные системы, включающие в себя программную и аппаратную части. При разработке методик (аппаратных комплексов) лаборатория должна сформулировать технические спецификации и требования, в соответствии с указанными ниже.

Если лаборатория приобретает готовое аналитическое (испытательное) оборудование в комплексе с компьютерными системами, прошедшее соответствующие законодательству валидации (аттестации), испытания и имеющее подтверждающие документы (свидетельства, сертификаты), с указанием аналитических функций (возможностей) требуемых лабораторией, то дополнительной (отдельной) валидации компьютерной системы в составе аналитического (испытательного оборудования) не требуется.

Валидация компьютерных систем в составе оборудования включает, но не ограничивается следующими уровнями.

Уровень I. Выбор программного обеспечения и компьютерного оборудования

Выбор и покупка нового программного обеспечения и связанного компьютерного оборудования должны следовать осознанному процессу принятия решений, основанному на требованиях целевого использования аналитического оборудования. Обычно, первым шагом, является выбор программного обеспечения, которое отвечает аналитическим требованиям предполагаемого использования. Типовые требования приведены ниже. На втором этапе, выбирают соответствующее компьютерное оборудование, которое отвечает всем аппаратным требованиям выбранного программного обеспечения. Типовые требования перечислены ниже.

Аналитические требования для программного обеспечения

— Алгоритмы интегрирования (обнаружение пика, идентификация, оценка параметров и т.д.)

— Алгоритмы калибровки

— Функции пригодности системы (фактор симметрии, теоретические тарелки, разрешение и т.д.)

— Статистические функции (среднее, стандартное отклонение и т.д.)

— Контроль аналитической системы

— Управление пользователями, то есть администрирование учетных записей пользователей и определение прав пользователей.

— Электронная подпись

— Совместимость с внешними программами (ЛИМС, Excel и т.д.)

Требования к аппаратной части

— Компоненты аппаратной части

— Операционная система

— Интерфейсы. Особое внимание следует обратить на характеристики АЦП, которые могут оказать влияние на разрешение, точность, линейность или частоту дискретизации (частоту отбора проб).

Для программного обеспечения и связанного компьютерного оборудования которое уже используется, требования к эксплуатационным характеристикам могут быть описаны ретроспективно.

Уровень II. Квалификация установки

Когда выбраны и куплены и программное обеспечение и компьютерное оборудование, вся система должна быть установлена и подключена к аналитическому прибору должным образом подготовленным персоналом. После установки, система должна быть надлежащим образом квалифицирована. Типичные параметры для тестирования приведены ниже.

Квалификации установки

— Верификация того, что установлена правильная операционная система (включая версию и пакет обновления).

— Верификация того, что программное обеспечение управляет аналитическим прибором.

— Верификация того, что измеряемые сигнал(ы) передается(ются) в программное обеспечение.

— Верификация правильного функционирования управления пользователями.

Уровень III. Квалификация функциональности программного обеспечения

Надлежащее функционирование программного обеспечения должно быть проверено путем тестирования производительности ключевых функций, таких как калибровка и количественное определение (внутренние стандарты, внешние стандарты), идентификация пика и расчет пригодности параметров системы.

В идеале, может быть использован набор исходных данных для которого известны результаты. Эти наборы исходных данных часто предоставляются поставщиком программного обеспечения. Они обрабатываются программным обеспечением и полученные результаты сравниваются с ожидаемыми значениями.

Если такие наборы данных недоступны, образец наборов исходных данных может быть получен путем прогона типичных образцов. Результаты обработанных наборов исходных данных должны быть проверены путем перерасчета основных параметров (например, калибровочные кривые по площадям пиков стандартов) с помощью стандартного программного обеспечения электронных таблиц.

III уровень квалификации необходимо повторять после установки новых модулей программного обеспечения, новых версий программного обеспечения, новых пакетов обновлений, патчей обновления или после серьезных изменений в структуре программного обеспечения компьютера (например новая антивирусная программа). Аналогичные действия следует предпринимать при каждом изменении аппаратной платформы.

Уровень IV. Пригодность для конкретной аналитической методики

В сочетании с валидацией аналитической методики, расчеты выполняемые с помощью программного обеспечения соответствующей компьютерной системы, также должны быть проверены. Особое внимание необходимо уделить группировке данных и статистическому анализу результатов. Во многих новых программах можно реализовать вычисления и контрольные поля определяемые пользователем. Правильное функционирование этих параметров должно быть проверено на собственном примере расчетов. Эти, определяемые пользователем, расчеты должны быть заблокированы или защищены паролем для предотвращения перезаписи.

В методике должны быть предусмотрены периодические проверки правильности проведения анализа (испытаний), которые будут подтверждать в том числе и пригодность компьютерной системы.

## 10. Планирование и документирование валидации ПО и компьютерных систем

В соответствии с требованиями ГОСТ Р 54360-2011 необходимо планировать и документировать процесс валидации. План валидации обеспечивает общее руководство процессом валидации. К плану валидации относятся, но неограничиваются ими, следующие пункты:

* Общие цели;
* Описание системы;
* Границы или допущения при испытаниях, согласно которым комиссия по валидации будет работать;
* Обязанности участников и основные инструкции для выполнения испытательных протоколов по квалификации монтажа (IQ) или квалификации функционирования(эксплуатации) (OQ).

План валидации должен включать перечень и описание всех компонентов программного обеспечения и аппаратных средств в соответствии с приложением 3. Иногда программные модули, ассоциированные с ЛИМС, изменяются при установке другого программного обеспечения. Эти изменения могут появляться при модернизации операционной системы, модернизации ЛИМС или других программ. Добавление компонентов аппаратных средств, видеокарт, модемов, звуковых карт и т.д. и связанных с ними типов программного обеспечения может затронуть состояние первоначальной валидации ЛИМС. Детальный перечень компонентов программного обеспечения и аппаратных средств, связанных с ЛИМС, является существенным, так как он представляет первоначальную конфигурацию ЛИМСи описывает первоначальное состояние, на котором базируется контроль над всеми изменениями. Все протоколы испытаний для квалификации монтажа и функционирования (IQ, OQ) связанных компонентов аппаратных средств и программного обеспечения включаются в план валидации. Последней частью плана валидации является подписание его лицами, ответственными за гарантирование того, что план валидации соответствует требованиям организации и нормативным требованиям. Обычно эти подписи включают подписи руководителя процессом валидации, являющегося уполномоченным лицом подразделения по обеспечению качества, руководителя лаборатории, менеджера ЛИМС и других лиц.

Испытание квалификации монтажа (IQ) должно основываться на спецификациях или рекомендациях производителя, или того и другого. Конфигурация конкретного приложения утверждается в качестве части испытания IQ, OQ.

Поставленные продавцом инструменты и методы диагностики могут быть использованы как часть испытания IQ, OQ. Протоколы испытания IQ, OQ, основанные на поставленных продавцом диагностиках, должны включать пошаговую проверку диагностических процедур, регистрацию всех результатов и критерии приемки каждого результата.

Документы протоколов IQ, OQ и результатов испытаний должны быть произведены для всех типов аппаратных средств и программного обеспечения, используемых ЛИМС: для операционной системы, базы данных, генератора отчета, статистических пакетов, сети, соединенных инструментов, компьютеров, включая терминалы, персональные компьютеры, клиентов, а также серверы, принтеры, плоттеры, считыватели штриховых кодов и т.д. Если приложение ЛИМС загружается в существующую компьютерную систему, может быть использована оригинальная документация квалификации монтажа (IQ) аппаратных средств. Предложенный формат протокола испытаний приведен в приложении 4

Протоколы валидационных испытаний необходимы для того, чтобы определить критические функции ЛИМС, которые будут испытываться. Критические функции ЛИМС должны базироваться на основных функциях и на намеченном для использования приложении ЛИМС. Должно быть предусмотрено разумное объяснение для того, чтобы не проводить тестирование каких-либо частей ЛИМС.

Разработка и выполнение протоколов испытаний (ПИ) в процессе валидации требуют большого количества времени. Этот факт часто игнорируется, когда разрабатывается проект плана валидации. На разработку протоколов испытаний и их выполнение влияют многие факторы. Во-первых, существенным является хорошая осведомленность о новой ЛИМС и о том, как она работает. Слабое ознакомление пользователя с ЛИМС приводит к более длительной разработке детальных протоколов испытаний. Команда по валидации должна выделить достаточное количество времени в календарном графике проектирования для персонала, разрабатывающего протоколы испытаний, чтобы он ознакомился с новой системой. Вторым фактором, влияющим на разработку протоколов испытаний, является то, насколько долго разработчик протоколов испытаний должен сосредоточиваться на проекте валидации. Недостаточная концентрация усилий по разработке протоколов испытаний добавит значительное количество дополнительных месяцев на проектирование валидации. На выполнение протоколов испытаний также существенно влияет сосредоточение внимания испытателя на выполнении протоколов испытаний. Третьим фактором, влияющим на разработку протоколов испытаний, является количество ресурсов, доступных для работы по протоколам испытаний. И последнее - уровень опыта лиц, пишущих и выполняющих протоколы испытаний, будет влиять на то, сколько времени понадобится для осуществления этих действий. По возможности, в организации должен быть по крайней мере один опытный сотрудник, взаимодействующий с теми, кто разрабатывает и выполняет протоколы испытаний.

Число протоколов испытаний, необходимых для валидации ЛИМС, зависит от сложности ЛИМС и уровня деталей, требуемых для адекватного испытания ключевых характеристик. Протоколы испытаний могут быть как простыми - один или два типа инструкций для выполнения, так и сложными - несколько сотен типов инструкций. Уровень сложности будет зависеть от направления, которого придерживается организация в проекте этих протоколов испытаний. Каждая организация должна иметь организационные СОП, которые описывают, как должны разрабатываться протоколы испытаний. Проект и основные инструкции, согласно которым должны действовать испытатели и чего они должны ожидать в качестве критерия приемки, могут быть как простыми, так и очень высокого уровня. Протоколы испытаний, созданные подобным образом, обычно требуют, чтобы испытатели описали в деталях, что именно они делали. На противоположной стороне спектра находятся те протоколы испытаний, которые инструктируют испытателей шаг за шагом о том, что именно им следует делать. Протоколы испытаний, разработанные подобным способом, обычно требуют от испытателей ответить: да/нет или истинный/ложный - относительно критериев приемки. В любом случае для выполнения и документирования сложных протоколов испытаний может потребоваться несколько дней. Детали, полученные испытателем относительно каждого протокола испытания, должны быть достаточными для того, чтобы гарантировать, что функции или процессы ЛИМС, которые испытываются, находятся под контролем (приложение 4).

В дополнение к выполнению протокола испытания команда по валидации должна предусмотреть достаточное количество времени, необходимого для рассмотрения результатов протокола испытания и решения любых конкретных проблем. Процесс рассмотрения может продолжаться почти так же долго, как выполнение протокола испытания, если испытание является чрезвычайно сложным. Количество времени, необходимое для того, чтобы выполнить этот этап валидации, часто недооценивается (занижается). Рассмотрение каждого протокола испытания необходимо для того, чтобы гарантировать, что его содержание обоснованно, а протокол испытаний придерживается требований к документации в соответствии с требованиями нормативных документов. В особенности должны быть предприняты единообразные действия относительно ошибок; испытатель должен подписать документ, поставить дату и привести причину, почему слово или группа слов были вычеркнуты. В некоторых случаях за принятие решения может быть ответственным рецензент, если протокол испытания успешно соответствует критериям приемки и, соответственно, принимается или отклоняется

Комиссия по валидации должна обратиться к валидационному плану относительно того, как она будет управлять протоколами несостоятельных (ошибочных) испытаний. Это должно быть сделано перед началом испытаний. Команда по валидации также должна сначала рассмотреть то, как будут вноситься изменения в протоколы испытаний после их утверждения уполномоченными специалистами по качеству. Возникают моменты, когда испытателям необходимо произвести изменения в протоколах испытаний в период фазы выполнения протоколов испытаний. Испытателями должен быть предусмотрен способ для включения этих изменений в существующий протокол испытаний. Процедура должна быть утверждена уполномоченными лицами по качеству и включена в план валидации. Дающаяся испытателю свобода должна быть использована для дальнейшего проектирования и следования этапам дополнительных испытаний в период выполнения процедуры испытаний. Эта свобода позволяет им исследовать, почему конкретный этап или ряд этапов не соответствует критериям приемки. Без этой свободы может быть отсрочен весь проект валидации.

Все протоколы испытаний должны быть разработаны для испытания установленных в ЛИМС характеристик или функций. Разработчики проекта протокола испытания может изъявить желание включить некоторые или все из следующих ниже характеристик в проекте протокола испытания.

Информация в заголовке протокола испытания

Эта секция содержит название организации, использующей ЛИМС, наименование отдела владельца ЛИМС, дату разработки протокола испытания, мотивировку, если протокол испытания предназначен для уполномоченных лиц по квалификации монтажа или функционирования, номер пересмотра протокола испытания и информацию о том, какая система испытывается (например, *"ABC" ЛИМС, версия 7.1*).

Каждый протокол испытания должен иметь уникальный идентификационный номер. Этот номер является уникальным лишь для связанного с планом валидации протокола испытания.

Цель. Протоколы испытаний разработаны для того, чтобы проводить различные испытания. Например, цель состоит в том, чтобы подтвердить, что информация о новых пользователях может быть добавлена, модифицирована или удалена из ЛИМС.

Требования. Имеются функциональные требования, которые испытываются по протоколу испытания. Протокол испытания может быть разработан для более чем одного функционального требования. Любое функциональное требование, которое не было включено в план валидации, не должно быть включено в разработку протоколов испытаний.

Специальные потребности или требования. В этом разделе перечисляются специальные пункты, которые необходимы для выполнения протокола испытания, включая специальные навыки, которые должен иметь испытатель, или связи с другими протоколами испытаний или другими приложениями.

Процедуры этапов испытания. Каждый этап испытания должен включать номер этапа, процедуру испытания и критерии приемки для этого этапа. Каждый этап испытания должен быть градуирован в соответствии с одной из трех категорий: испытание в обычных условиях (normal testing); испытание в предельных режимах (stress testing); испытание надежности (robustness testing).На этапах испытания в обычных условиях проверяется функция ЛИМС с использованием всех общих пользовательских команд. Этапы испытаний, которые проверяют функцию в ее границах, являются испытаниями в предельных режимах (нагрузочными испытаниями). Примером может являться *введение 20 символов в 20 символьных полей*. Испытание надежности (устойчивости) представляет собой испытание характеристик за пределами их границ. Например, *пароль пользователя может принимать только текстовые знаки или числа, однако испытатель отдает распоряжение для введения специальных знаков или знаков пунктуации для недавно созданного пароля пользователя*. Испытатели должны определить, прошел ли этап испытания критерии приемки. Обычно это выражается простым утверждением: **да/нет.**

Раздел комментариев. Данный раздел используется испытателями для введения их комментариев по поводу любых неожиданных результатов, полученных в процессе выполнения протокола испытания. Пользователи также могут отмечать, как эти неожиданные результаты объясняются.

Завершение работы испытателя. Испытатель должен подписать и датировать протокол испытания в конце процесса испытания. Если протокол испытания занимает несколько страниц, испытателю следует подписать и датировать ту страницу, на которой указано, когда они завершили этапы испытаний. В некоторых организациях испытатели ответственны за принятие решения в отношении того, проходят ли или терпят неудачу испытания. Если испытания не выполнены, испытатели должны документировать в разделе комментариев, почему испытания не были выполнены. Если испытатели приняли какое-либо решение, они также должны его документировать.

Завершение работы рецензента. Рецензент протокола испытания должен подписать и датировать протокол испытания только после рассмотрения данных и подтверждения того, что протокол испытания завершен. Если имеются вопросы, рецензент не должен подписывать протокол испытания, пока на эти вопросы не будут получены ответы. В некоторых случаях рецензент несет ответственность за принятие решения относительно того, выполнен или не выполнен протокол испытания. Если протокол испытания не выполнен, рецензент должен использовать раздел комментариев, чтобы объяснить в нем, почему это произошло. Рецензент не должен осуществлять каких-либо изменений в документе. Если изменения должны быть внесены, необходимо связаться с основным испытателем, чтобы осуществить эти изменения.

Приложения. Все приложения, которые являются частью выполнения протокола испытания, должны содержать следующую информацию: идентификационный номер протокола испытания; номер этапа; информацию о тех, кто создал приложение; дату, когда приложение было создано. Кроме того, испытатель может изъявить желание выдвинуть на первый план или объяснить отдельные пункты приложения. Любое рукописное изменение, внесенное в отдельный пункт, должно следовать тем же самым критериям, что и протокол испытаний, и включать единообразные действия по оформлению этого пункта, информацию о лице, производящем изменения, дату и причину внесения изменения.

Как только завершается оформление протоколов испытаний, они должны быть отправлены на рассмотрение. После того как они будут рассмотрены и подписаны, они должны быть переданы руководителю комиссии по валидации. Это облегчит разработку заключительного валидационного отчета. Кроме того, если принимались меры по поводу аварийных отключений идентифицируемой системы, руководитель комиссии по валидации может начать рассмотрение этих проблем, не препятствуя дальнейшей деятельности членов команды по испытаниям.

Члены комиссии по валидации могут использовать несколько подходов для решения задач по проектированию и испытанию внедрения ЛИМС. Команда по испытаниям может выразить желание включить следующие дополнительные варианты подходов в проект протоколов испытаний.

1. Управление поставляемыми продавцом диагностическими тестами (*поставляемый комплект компонентов/тестов нуждается в валидации перед их использованием*).
2. Управление автоматизированными средствами испытания, если они доступны, конкретной ЛИМС (*поставляемый комплект компонентов/тестов нуждается в валидации перед их использованием*).
3. Регистрация результатов вручную, наряду с ЛИМС, для данного периода времени, и сравнение результатов.
4. Следует ввести ошибки преднамеренно и определить, идентифицирует ли их система должным образом или отклонит их.
5. Следует нагрузить систему искусственно и полностью заполнить ее данными или работать с многими действиями сразу.
6. Если функционирование происходит в среде Windows, то, например, следует открыть все окна сразу.
7. Следует запланировать загрузки больших массивов информации.
8. Следует испытать безопасность путем попытки прерывания или использования запрещенных функций. Следует рассмотреть скрытые алгоритмы входа.
9. Следует попытаться прервать вход, чтобы посмотреть, будет ли система вести себя особым образом.
10. Следует визуально осмотреть интерфейсы и другие компоненты системы, которые производят существенные действия.
11. Следует изменять последовательность загрузки автоматизированных инструментов.
12. Для полноты исследования следует рассмотреть каждый выводящий экран, исправить данные в каждом поле и четко следовать спецификации.
13. Следует использовать технику захвата экрана или технику одновременного нажатия клавиш, чтобы рассмотреть работу системы.
14. Следует испытать все события запусков, принуждая систему к выполнению этих действий. Следует включать класс запланированных событий и в максимально возможной степени класс событий исключения.
15. Следует отключить источник питания от инструментов, связанных интерфейсами, от серверов и других частей системы.
16. Следует использовать протоколы испытаний для исследования работы сети, включая следование протоколу, временным границам и целостности данных.
17. Следует использовать симуляторы инструментов, если таковые имеются в распоряжении, для проверки особых ситуаций и ошибок в интерфейсах.

После того как ЛИМС будет валидирована, начинается эксплуатационное обслуживание системы. На этом этапе члены комиссии по валидации могут быть распущены.

## 11. Эксплуатация ПО

Конкретная установка заканчивается после валидации программного обеспечения. Оператор подписывает журнал жизненного цикла ПО подтверждающий правильную установку. Этот журнал, который фактически является документом учета и обеспечения качества, включает в себя название программного обеспечения, уникальный идентификатор, локализацию, а также лицо ответственное за программное обеспечение. Он также включает в себя верификацию и другие спецификации, обновления или какие-либо замеченные проблемы. Верификация завершается после установки и отображается в журнале жизненного цикла ПО (приложение 7).

В журнале жизненного цикла ПО необходимо регистрировать эксплуатационные отчеты, сведения о резервном копировании, частичном резервировании. Отдельно должны вестись записи об ошибках и принятых решениях, запросы на обслуживание, а также запросы на изменения (приложение 8).

|  |  |  |  |
| --- | --- | --- | --- |
| **Информация/документация, которая должна быть доступна** | **Коммерческое ПО** | **ПО Собственной разработки** | **Специальные документы** |
| Название, версия и уникальный идентификатор ПО | X | X | Журнал жизненного цикла ПО и распечатки |
| Оригинальные файлы (CD-ROM …) или место хранения для установки ПО и ПО для управления компьютерным окружением | X | X | Резервное копирование программного обеспечения в сети |
| Дата ввода ПО в эксплуатацию | X | X | Журнал жизненного цикла ПО |
| Текущее физическое местоположение, если необходимо | X | X | Журнал жизненного цикла ПО |
| Ответственное лицо, отвечающее за программное обеспечение |  | X | Журнал жизненного цикла ПО |
| Условия, при которых программа запускается в работу, если это потребуется (аппаратное обеспечение, операционная система, …) | X | X | Не применяется |
| Имя лица, разработавшего и валидировавшего ПО, а также дата валидации |  | X | Сертификат валидации |
| Исходный код, если доступен |  | X | Распечатка формул |
| Правила эксплуатации, при необходимости |  | X | Не подходит |
| Документация по регулярной верификации ПО | X | X | Журнал жизненного цикла ПО, Отчеты по верификации |
| Документация по валидации ПО | X | X | Файл валидации ПО |
| Порядок действий при возникновении сбоев, поддержание рабочего процесса, обновление версий и, при необходимости, управления конфигурациями | X | X | Журнал жизненного цикла ПО |

**Контроль изменений.** То, что ЛИМС или иное ПО изменяются, является естественным процессом. Однако в обязательном порядке все осуществленные изменения должны пройти контроль изменений. Необходимо ограничить доступ к настройкам и изменениям ЛИМС и другого ПО, пользователей, которые по должностным обязанностям не отвечают за функционирование ПО.

Контроль изменений включает несколько этапов: запрос на изменение; анализ воздействия; рассмотрение/утверждение; внедрение; валидирование. Кроме того, организация должна иметь персонал, контролирующий изменения, который рассматривает все предложенные средства для контроля изменений. К этому персоналу относятся персонал подразделения по обеспечению качества, знакомый с валидацией компьютерных систем, и персонал, относящийся к различным отделам лаборатории. Персонал рассматривает и оценивает воздействия изменения на функционирование ЛИМС. Готовясь принимать решение относительно требований к изменению ЛИМС, следует рассмотреть следующее: будут ли изменения обеспечивать достаточно большие преимущества, чтобы возместить время и ресурсы, необходимые для повторной валидации ЛИМС; на какие другие системы будет воздействовать изменение; сколько времени потребуется для успешного внедрения изменения; какие ресурсы должны быть доступны, чтобы осуществить изменение; какие воздействия не будут приводить к изменениям как в лаборатории, так и в организации. Изменения необходимо отражать в спецификациях пользователя на ПО. Если изменения касаются добавления новых ранее не документированных и не валидированных функций, требуется повторная валидация, с внесением изменений в план и протоколы валидации. При изменении документированных и валидированных функций, достаточно провести испытания этих функций при периодической или внеочередной верификации как указано ниже.

С целью контроля необходимо проводить периодический аудит и верификацию ПО и компьютерных систем. Объем и сроки повторной верификации определяется характером и количеством обнаруженных при эксплуатации ошибок, периодичностью обслуживания, наличием внеплановых обслуживаний, доработками и обновлениями со стороны поставщиков (разработчиков) ПО, запросами на изменения.

Верификация проводится по протоколам испытаний, созданных при валидации, некоторые шаги протокола испытаний могут быть пропущены, если по этому функционалу не возникали ошибки либо данный функционал не используется в работе (отсутствуют рабочие записи). Ответственные за испытания должны делать соответствующие отметки в протоколе испытаний.

### **Приложение 1**

*Сведения об организации и лаборатории*

*Утверждение*

**Протокол** валидации/верификации расчетов в программах электронных таблиц и другом ПО

№\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_г

в дополнение к протоколу валидации №\_\_\_ от \_\_\_\_\_\_\_г *(в случае верификации)*

Используемое программное обеспечение (ПО, наименование и версия, идентификатор): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Методика, НД, содержащий формулу | Формула *(например х=(y-a)/k)* | Переменные в формуле и соответствующие им числовые значения от 2 до 20.  *(например - y = 2; a = 3; k = 4)* | Результат ручного пересчета | Результат из ПО | Заключение (соответствует/несоответствует) |

Заключение о валидации ПО (соответствует/не соответствует)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Местонахождение проверенного экземпляра \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Приложения *(если есть)*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Исполнитель \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись ФИО

Дата: \_\_\_\_\_\_\_\_\_\_\_\_

### **Приложение 2**

*Сведения об организации и лаборатории*

*Утверждение*

ИНФОРМАЦИЯ ПО ОЦЕНКЕ ПРОДАВЦА

(образец формы)

|  |  |
| --- | --- |
| Наименование продукта |  |
| Наименование продавца |  |
| Контактная информация |  |
| Оценка (итоговая) |  |
| Кем проведен аудит: |  |
|  |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Пункты аудита | Уровень информации о свидетельстве:  1 - не имеется,  2 - некоторая,  3 - полная | Комментирующие/ссылочные документы |
| Разработка программного обеспечения |  |  |
| Рассмотрение стандартов/руководств/процедур(жизненный цикл программных средств) |  |  |
| Свидетельство о технических экспертизах |  |  |
| Свидетельство о методах стандартной кодировки |  |  |
| Разрабатываемая документация существует для: |  |  |
| Фаза требований |  |  |
| Фаза проекта |  |  |
| Фаза исходного кода |  |  |
| Фаза испытания |  |  |
| Фаза установки и проверки |  |  |
| Фаза эксплуатации и обслуживания |  |  |
| Структура модуля исходного кода: |  |  |
| Информация в заголовке |  |  |
| Наименования программы |  |  |
| Описание программы |  |  |
| Штамп с датой и временем разработки |  |  |
| Имя (имена) разработчика(ов) |  |  |
| Входные сигналы |  |  |
| Выходные сигналы |  |  |
| Вызовы программы и подпрограммы |  |  |
| Параметры данных |  |  |
| Сектор пересмотра - контроля |  |  |
| Аннотированный код |  |  |
| Испытание |  |  |
| Структурное испытание (испытания кода) |  |  |
| Функциональное испытание (испытания проекта) |  |  |
| Комплекты данных валидационных испытаний |  |  |
| Документированные результаты и исключения, полученные при испытании |  |  |
| Обслуживание программного обеспечения |  |  |
| Настройка стандартного программного обеспечения |  |  |
| Контроль пересмотра |  |  |
| Синхронизация между продавцом и клиентом |  |  |
| Контроль конфигурации |  |  |
| Качество программного обеспечения и проблемы контроля |  |  |
| Группа обеспечения качества программного продукта |  |  |
| Контроль безопасности для доступа к программному обеспечению |  |  |
| Процедуры по обнаружению ошибок и разрешению внутренних проблем и выходные записи |  |  |
| Управление распределением |  |  |
| Записи для сохранения графиков |  |  |
| Аварийное восстановление |  |  |
| План по качеству программного обеспечения |  |  |
| Функциональные требования к программному обеспечению |  |  |
| Качество программного обеспечения и контроль проблем |  |  |
| Разработка жизненного цикла программного обеспечения |  |  |
| Требования к программному обеспечению по обучению разработчика |  |  |
| План валидации программного обеспечения |  |  |
| Общие проблемы объекта |  |  |
| Контроль безопасности для доступа в здание |  |  |
| Общая чистота |  |  |
| Организационные проблемы качества и контроля |  |  |
| Стандартные операционные процедуры (на уровне организации или отдела) |  |  |
| Применение СОП |  |  |
| Программа обучения |  |  |
| Записи о персональной квалификации |  |  |
| Записи о персональном обучении |  |  |
| Записи о контрактном обучении/контролю программистов |  |  |
| Программа внутреннего аудита |  |  |
| Политика в области качества |  |  |
| Руководство (инструкция) по качеству |  |  |
| Контроль документации |  |  |
| Модель жизненного цикла продукта |  |  |
| План проекта продукта |  |  |

Исполнитель \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись ФИО

Дата: \_\_\_\_\_\_\_\_\_\_\_\_

### **Приложение 3**

*Сведения об организации и лаборатории*

*Утверждение*

*дата*

ПЛАН ВАЛИДАЦИИ

*(образец формы)*

Валидируемое программное обеспечение (ПО, наименование и версия, идентификатор): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Вводная часть плана**

1) Цель валидации:

*соответствие требованиям НД (перечислить), соответствие требованиям спецификаций ТЗ, оценка текущего состояния, проверка расчетов.*

2) Описание спецификаций системы:

*Сведения о спецификациях из ТЗ и описаний поставщика.*

3) Допущения и границы испытания

*Сведения о требованиях к системе (спецификации), которые должны быть проверены.*

4) Ответственные за валидацию

Члены комиссии:

Привлекаемые лица:

*(список участвующих в работе лиц; их должности, ответственность и положение в комиссии).*

5) Отчет разработки:

*(Отчет разработчика об испытаниях и результатах - относится к системам собственной разработки).*

6) Основные инструкции:

*(должны быть представлены подробные инструкции путем включения ссылок на то, как выполнять испытания по квалификации монтажа и функционирования IQ/OQ).*

**Квалификация монтажа (IQ)**

(*включает установленные документированные свидетельства о том, что ЛИМС устанавливается и конфигурируется в соответствии с целью проекта и требованиями пользователя. Квалификация монтажа IQ обычно не включает эксплуатацию системы).*

7) Список и описание оборудования:

*(список всех наиболее важных компонентов аппаратных средств и программного обеспечения с кратким описанием функций и структуры каждого из них. Этот список должен включать дату выпуска, модель и число пересмотров компонентов соответственно).*

8) Технические спецификации:

(должны включать любые спецификации компонентов, необходимых для эффективной установки системы или подсистемы).

(блок-схемы, модели данных и т.д. - все то, что дает четкое представление о системе или подсистеме).

9) Требования к окружающей среде

(обсуждаются элементы того, что существует вне ЛИМС, но необходимо для эффективной эксплуатации системы. Эти элементы должны включать требования к энергоснабжению, кондиционированию воздуха, другому программному обеспечению, другим аппаратным средствам, то есть всему тому, что необходимо для функционирования ЛИМС).

10) План и протокол испытания квалификации монтажа (IQ)

*(здесь приводятся детали плана испытания для того, чтобы подтвердить, что ЛИМС установлена и конфигурирована в соответствии с проектом и требованиями пользователя. План испытания должен представить обоснованную инструкцию для оценки того, что задача выполнена корректно. Каждый план и протокол должны включать требование(я), подлежащее испытанию, процедуры испытания и критерии приемки для каждой процедуры испытания).*

*A) Первоначальные процедуры настройки*

*В) Критерии испытания*

*C) Процедуры испытания*

Таблица согласованных процедур испытания\*:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Процедура | Вид испытания | Критерий приемки |
|  |  |  |  |

\*Таблица может дополняться по мере заполнения протокола испытания

**Квалификация эксплуатации (функционирования) (OQ)**

*(должна включать установленные документированные свидетельства того, что ЛИМС функционирует в соответствии с предусмотренными диапазонами. Эта деятельность требует оценки ЛИМС в соответствии с динамическими эксплуатационными условиями. Не требуется повторять полную квалификацию эксплуатации при каждой новой установке, пока установка проводится в пределах первоначально квалифицированных эксплуатационных диапазонов и функциональных требований. Требуется, однако, проведение ограниченной квалификации функционирования)*.

11) Наиболее важные факторы:

*(список наиболее важных факторов для ЛИМС, определенных в процессе проектирования и разработки на основании информации продавца или технических решений. Перечисленные критические факторы должны быть верифицированы в соответствии с планом испытаний).*

12) План и протокол испытания квалификации функционирования или эксплуатации (OQ):

*(здесь должны быть приведены детали плана испытания для того, чтобы верифицировать, что ЛИМС установлена и конфигурирована в соответствии с проектом и требованиями пользователя. План и протокол испытания должны представить обоснованную инструкцию для оценки того, что задача выполнена корректно. План и протокол испытания должны определить ожидаемые результаты и критерии приемки для каждого критического фактора или функции. Испытание выполняется не только в ожидаемых границах вводимых значений и объемов (испытания в обычных условиях), но также проверяется, как ЛИМС будет реагировать на испытание эксплуатации в неожиданных или экстремальных диапазонах и условиях (испытание в предельных режимах), а также на испытание эксплуатации в заведомо некорректных диапазонах и условиях (испытание надежности и устойчивости).*

*Х. Описание валидируемой функции, модуля или части ЛИМС.*

Таблица согласованных процедур испытания\*:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Процедура | Вид испытания | Критерий приемки |
|  |  |  |  |

\*Таблица может дополняться по мере заполнения протокола испытания

13) Отчеты по валидации расчетов в ПО (модулях ЛИМС)

**Приложения:** *сертификаты, спецификации поставщика, информация по оценке поставщика*

**Подписи**

*(этот пункт должен включать информацию о том, кто представляет на рассмотрение план команды по валидации, персональные сведения о лицах, ответственных за рецензирование валидационного документа, и подтверждение того, что валидация была завершена корректно. Обычно эти подписи включают данные, полученные от уполномоченных специалистов организации по гарантии качества, сотрудников лаборатории, ответственных за ЛИМС, представителей группы управления информацией).*

### **Приложение 4**

*Сведения об организации и лаборатории*

*Утверждение*

*дата*

**Протокол** валидации/верификации ПО

№\_\_\_\_\_\_\_

Используемое программное обеспечение (ПО, наименование и версия, идентификатор): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Х. Испытываемая функция, модуль или часть ЛИМС*

*описание целей и требований валидации*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Процедура | Вид испытания | Критерий приемки | Соответствие  да/нет | Примечание |
|  |  |  |  |  |  |

Соответствует критериям приемки: ДА / НЕТ

Приложение: отчет об ошибках валидации/функционирования на \_\_\_\_ л.

Комментарии испытателя:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Испытано кем

\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись ФИО

Дата: \_\_\_\_\_\_\_\_\_\_\_\_

Комментарии рецензента: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Рецензировано кем \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись ФИО

Дата: \_\_\_\_\_\_\_\_\_\_\_\_

### **Приложение 5**

*Шапка*

*Утверждение*

*дата*

Отчет об ошибках при валидации

*Х. Испытываемая функция, модуль или часть ЛИМС*

*описание возникших ошибок и обстоятельств их возникновения.*

*Приложение: скриншоты, распечатки со сведениями об ошибках на \_\_\_\_ л.*

Комментарии испытателя:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Испытано кем \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись ФИО

Дата: \_\_\_\_\_\_\_\_\_\_\_\_

Комментарии рецензента: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Рецензировано кем \_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись ФИО

*Дата: \_\_\_\_\_\_\_\_\_\_\_\_*

### **Приложение 6**

*Сведения об организации и лаборатории*

*Утверждение*

*дата*

**Заключительный отчет о валидации**

Валидируемое программное обеспечение (ПО, наименование и версия, идентификатор): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Ссылка на план валидации (номер и дата)**

Ответственные за валидацию

**Члены комиссии:**

**Привлекаемые лица:**

*(список участвующих в работе лиц; их должности, ответственность и положение в комиссии).*

**Даты проведения валидации системы**

**Результаты валидации системы:**

*Количество проверок (протоколов тестирования). Обнаруженные ошибки, степень критичности ошибок.*

**Заключение по валидации системы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Установленный период ревалидации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Приложения к отчету:** *протоколы испытаний, отчеты об ошибках*

**Подписи комиссии**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Дата \_\_\_\_\_\_\_\_\_\_\_\_\_\_

### **Приложение 7**

Журнал жизненного цикла ПО

ПО, наименование и версия, идентификатор:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Производитель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Контакты ТП \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Место установки ПО \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ответственный за ПО \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Дата | Обнаруженные ошибки | Действия (обновления) | Комментарий | Ответственный | Подпись |
|  |  |  |  |  |  |

### **Приложение 8**

**Журнал обращений пользователей ПО**

***(багтрекер)***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Д**ата | Наименование проблемы | Сотрудник | Описание проблемы | Решение проблемы | Срок решения | Разработчик |
| ‍ |  |  |  |  |  |  |

### **Приложение 9**

**Лист ознакомления**

|  |  |  |
| --- | --- | --- |
|  | **ФИО** | **Подпись** |
| **Разработал:** |  |  |
| **Проверил:** |  |  |
| **Согласовано МК** |  |  |