МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 31887— 2012

ПРИНЦИПЫ НАДЛЕЖАЩЕЙ ЛАБОРАТОРНОЙ ПРАКТИКИ (GLP)

Применение Принципов GLP к компьютеризированным системам

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

Цели, основные принципы и основной порядок проведения работ по межгосударственной стандартизации установлены в ГОСТ 1.0—2015 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2—2015 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский центр стандартизации, информации и сертификации сырья, материалов и веществ» (ФГУП «ВНИЦСМВ»); Техническим комитетом по стандартизации № 339 «Безопасность сырья, материалов и веществ» Федерального агентства по техническому регулированию и метрологии; Межгосударственным техническим комитетом по стандартизации МТК 339 «Безопасность сырья, материалов и веществ»

2 ВНЕСЕН Федеральным агентством по техническому регулированию и метрологии

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 9 ноября 2012 г. № 53-П)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Армения	AM	Минэкономики Республики Армения
Беларусь	BY	Госстандарт Республики Беларусь
Казахстан	KZ	Госстандарт Республики Казахстан
Киргизия	KG	Кыргызстандарт
Молдова	MD	Молдова-Стандарт
Россия	RU	Росстандарт
Таджикистан	TJ	Таджикстандарт

4 Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2012 г. № 2153-ст межгосударственный стандарт ГОСТ 31887—2012 введен в действие в качестве национального стандарта Российской Федерации с 1 января 2013 г.

5 Настоящий стандарт идентичен международному документу из серии документов Организации экономического сотрудничества и развития (ОЭСР) о Принципах GLP и мониторинге соответствия. Консенсусный документ по GLP. Применение Принципов надлежащей лабораторной практики к компьютеризированным системам: 1995, № 10 (OECD series on Principles of Good Laboratory Practice and Compliance Monitoring — No 10 — GLP consensus document — The application of the principles of GLP to computerized systems: 1995, IDT). При этом все разделы полностью идентичны, а термины и определения из приложения перенесены в раздел «Термины и определения».

Международный документ разработан Рабочей группой ОЭСР по GLP.

Наименование настоящего стандарта изменено относительно наименования указанного международного документа в связи с особенностями построения межгосударственной системы стандартизации

6 ВВЕДЕН ВПЕРВЫЕ

7 ПЕРЕИЗДАНИЕ. Сентябрь 2018 г.

*Информация об изменениях к настоящему стандарту публикуется в ежегодном информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2018

В Российской Федерации настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Термины и определения 1
3 Применение Принципов GLP к компьютеризированным системам 2
3.1 Общие положения 2
3.2 Принципы GLP и компьютеризированные системы 2
Библиография 9

Введение

В рамках третьего консенсусного симпозиума Организации экономического сотрудничества и развития (ОЭСР) по надлежащей лабораторной практике (GLP), состоявшегося 5—8 октября 1992 г. в Интерлакене (Interlaken), Швейцария, Рабочая группа экспертов обсудила вопрос об интерпретации Принципов GLP применительно к компьютеризированным системам. Председателем Рабочей группы был доктор Тео Хелдер (Dr. Theo Helder), представитель органа мониторинга соответствия Принципам GLP Нидерландов, в качестве докладчика симпозиума выступал Брайан Доэрти, председатель Вычислительного комитета Британской ассоциации обеспечения качества научно-исследовательских работ (Mr. Bryan Doherty, Chairman of the Computing Committee of the British Association for Research Quality Assurance).

Участниками Рабочей группы были представители как национальных органов мониторинга соответствия Принципам GLP, так и испытательных лабораторий Австрии, Бельгии, Дании, Финляндии, Франции, Германии, Японии, Нидерландов, Швейцарии, Великобритании и США, которые в отведенное для обсуждения время не смогли достичь консенсуса относительно подробного руководящего документа. Однако данная Рабочая группа разработала документ, озаглавленный «Концепции в области GLP, относящиеся к компьютеризированным системам», в котором изложены основные принципы и описаны проблемы, связанные с ними. Данный документ был направлен странам — членам ОЭСР для комментариев.

В свете полученных комментариев Группа по GLP на пятом совещании в марте 1993 г. приняла решение о необходимости проведения дальнейшей работы и предусмотрела второе заседание Рабочей группы, которое состоялось 14—16 декабря 1994 г. в Париже под председательством д-ра Хелдера (Dr. Helder), с участием господина Доэрти (Mr. Doherty) в качестве докладчика, а также участием представителей правительств и промышленности Канады, Дании, Франции, Германии, Японии, Нидерландов, Швеции, Великобритании и Соединенных Штатов Америки.

Проект разработанного Рабочей группой консенсусного документа основывается на документе, рассмотренном на симпозиуме в Интерлакене, комментариях стран — членов ОЭСР к нему и документе, разработанном совместной правительственно-промышленной Рабочей группой Великобритании. Впоследствии он был пересмотрен, изменен и одобрен Рабочей группой, участниками совместного совещания Группы по химическим веществам и Управляющего комитета специальной программы по контролю химических веществ. На основании этого Комитет по экологической политике рекомендовал снять с данного документа гриф секретности под эгидой генерального секретаря.

М Е Ж Г О С У Д А Р С Т В Е Н Н Ы Й С Т А Н Д А Р Т

ПРИНЦИПЫ НАДЛЕЖАЩЕЙ ЛАБОРАТОРНОЙ ПРАКТИКИ (GLP)

Применение Принципов GLP к компьютеризированным системам

Principles of Good Laboratory Practice (GLP). Application of GLP Principles to computerised systems

Дата введения — 2013—01—01

1 Область применения

1.1 Настоящий стандарт устанавливает требования к управлению компьютеризированными системами, используемыми при проведении исследований в испытательных центрах, функционирующих в соответствии с требованиями Принципов надлежащей лабораторной практики (GLP).

На протяжении последних лет возрастает использование компьютеризированных систем испытательными центрами, в которых проводят испытания химических веществ для оценки их безопасности для здоровья человека и окружающей среды. Компьютеризированные системы могут быть предназначены для прямого или непрямого сбора данных, их обработки, представления и хранения, и они все чаще являются составной частью автоматизированного оборудования.

1.2 Все компьютеризированные системы, используемые для производства, измерения или оценки данных, предназначенных для представления в соответствующие регулирующие органы, должны разрабатываться, валидироваться, эксплуатироваться и обслуживаться в соответствии с Принципами Организации экономического сотрудничества и развития (ОЭСР) по (GLP) [1].

В ходе планирования и проведения исследований, а также создания отчетов для различных целей может использоваться несколько компьютеризированных систем. К таким целям могут относиться прямой или непрямой сбор данных с автоматизированных приборов, эксплуатация/управление автоматизированным оборудованием, а также обработка, представление и хранение данных. Для подобных различных видов деятельности компьютеризированные системы могут варьироваться от программируемого аналитического прибора или персонального компьютера до многофункциональной лабораторной информационной менеджмент-системы (ЛИМС). Принципы GLP следует применять независимо от масштаба привлечения средств автоматизации.

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

2.1 **критерии приемки** (acceptance criteria): Документированные критерии, которым необходимо соответствовать для успешного завершения этапа испытания или выполнения требований поставки.

2.2 **приемочные испытания** (acceptance testing): Выполненное по установленной форме испытание компьютеризированной системы в предполагаемой рабочей среде с целью определения соответствия критериям приемки испытательного центра, а также приемлемости системы для эксплуатации.

2.3 **резервное копирование** (back-up): Меры, предпринимаемые для восстановления файлов данных и программного обеспечения, возобновления обработки данных или использования альтернативного компьютерного оборудования после системного сбоя или аварии.

2.4 **контроль изменений** (change control): Постоянная оценка и документирование системных операций и изменений с целью определения необходимости процесса валидации после появления в компьютеризированной системе каких-либо изменений.

Издание официальное

2.5 **компьютеризированная система** (computerised system): Группа компонентов аппаратных средств и связанного с ними программного обеспечения, разработанных и собранных для выполнения определенной функции или группы функций.

2.6 **электронная подпись** (electronic signature): Запись в виде магнитных импульсов или трансляция (компиляция) компьютерных данных любого символа или последовательностей символов, выполняемых, адаптированных или авторизованных определенным лицом в качестве эквивалента собственноручной подписи данного лица.

2.7 **аппаратное обеспечение** (hardware): Физические компоненты компьютеризированной системы, включая как сам компьютер, так и его периферийные компоненты.

2.8 **периферийные компоненты** (peripheral components): Любое связанное с помощью интерфейса оборудование или вспомогательные или удаленные компоненты, такие как принтеры, модемы, терминалы и т. д.

2.9 **общепризнанные технические стандарты** (recognised technical standards): Стандарты, распространенные национальными или международными органами по стандартизации [ISO, International organization for standartization (Международная организация по стандартизации, ИСО); IEEE, Institute of Electrical and Electronics Engineers (Институт инженеров по электротехнике и электронике), ANSI, American National Standards Institute (Американский национальный институт стандартов) и т. д.].

2.10 **безопасность** (security): Защита компьютерного аппаратного и программного обеспечения от случайного или предумышленного доступа, использования, модификации, уничтожения или разглашения. Также безопасность относится к персоналу, данным, коммуникационным связям и физической и логической защите компьютерных инсталляций.

2.11 **программное обеспечение — приложение** (software — application): Программа, приобретенная или разработанная, адаптированная или приспособленная к требованиям испытательных центров с целью контроля процессов сбора, обработки, представления данных и/или архивирования.

2.12 **программное обеспечение — операционная система** (software — operating system): Программа или набор программ, стандартных (рутинных) программ и подпрограмм, контролирующих работу компьютера. Операционная система может предоставить услуги, такие как распределение ресурсов, планирование работ, управление вводом/выводом и управление данными.

2.13 **исходный код** (source code): Оригинальная компьютерная программа, выраженная в пригодной для чтения человеком форме (язык программирования), которую необходимо перевести в машиночитаемую форму, прежде чем она может быть выполнена компьютером.

2.14 **валидация компьютеризированной системы** (validation of a computerised system): Подтверждение того, что компьютерная система подходит для предусмотренной области применения.

3 Применение Принципов GLP к компьютеризированным системам

3.1 Общие положения

Компьютеризированные системы, связанные с проведением исследований, предназначенных для представления в регулирующие органы, должны иметь соответствующую конструкцию, достаточную мощность и подходить для реализации их предназначения. Системы должны разрабатываться, валидироваться и эксплуатироваться в соответствии с Принципами GLP, кроме того, должны быть установлены соответствующие процедуры контроля и технического обслуживания данных систем. Подтверждение того, что компьютеризированная система соответствует своему назначению, имеет фундаментальное значение и называется «компьютерная валидация».

Процесс валидации обеспечивает высокую степень уверенности в соответствии компьютеризированной системы заранее заданным техническим требованиям. Валидация должна осуществляться до начала эксплуатации системы и проводиться надлежащим образом только с помощью разработанного плана валидации.

3.2 Принципы GLP и компьютеризированные системы

При применении Принципов GLP к вышеописанным компьютеризированным системам следует принимать во внимание требования 3.2.1—3.2.9.

3.2.1 Обязанности и ответственность

а) Администрация испытательного центра несет полную ответственность за соблюдение Принципов GLP, включая назначение на должность и эффективную организацию достаточного числа квалифи-

цированных и опытных сотрудников, а также обязана обеспечивать, чтобы помещения, оборудование и процедуры обработки данных находились на должном уровне.

Администрация испытательного центра несет ответственность за обеспечение соответствия компьютеризированных систем предполагаемому назначению. Она должна устанавливать принципы организации и процедуры в области автоматизации, гарантирующие разработку, валидацию, эксплуатацию и обслуживание систем в соответствии с Принципами GLP.

Администрация испытательного центра должна обеспечивать ясность и соблюдение данных принципов организации и процедур, а также эффективный контроль выполнения данных требований.

Администрация испытательного центра должна назначать сотрудников, несущих конкретную ответственность за разработку, валидацию, эксплуатацию и обслуживание компьютеризированных систем. Данный персонал должен иметь соответствующую квалификацию, опыт и достаточную подготовку для выполнения своих обязанностей в соответствии с Принципами GLP.

b) Руководители исследования согласно Принципам GLP несут ответственность за общее проведение исследований.

Поскольку для проведения многих подобных исследований будут использоваться компьютеризированные системы, важно, чтобы руководители исследования в полной мере осознавали их использование в исследовании для достижения определенной цели.

Ответственность руководителя исследования относительно данных, полученных в электронном виде, идентична ответственности при работе с данными, хранящимися на бумажном носителе. Кроме того, в исследованиях GLP следует использовать только системы, прошедшие процедуру валидации.

c) Персонал

Весь персонал, использующий компьютеризированные системы, несет ответственность за эксплуатацию данных систем в соответствии с Принципами GLP. Сотрудники, которые разрабатывают, валидируют, эксплуатируют и обслуживают компьютеризированные системы, несут ответственность за выполнение вышеперечисленных мероприятий в соответствии с Принципами GLP и установленными техническими нормами.

d) Обязательства и ответственность службы обеспечения качества в отношении компьютеризированных систем должны определяться администрацией испытательного центра и описываться служебными инструкциями и процедурами. Программа обеспечения качества должна включать в себя процедуры и методы, гарантирующие соответствие всех этапов валидации, эксплуатации и технического обслуживания компьютеризированных систем установленным стандартам. Кроме того, программа должна включать в себя процедуры и методы установки приобретенных систем и процесс разработки компьютеризированных систем внутренними силами организации.

Персонал службы обеспечения качества призван контролировать соответствие компьютеризированных систем Принципам GLP и должен получить обучение необходимым специальным (профильным) техническим навыкам. Сотрудники службы обеспечения качества должны быть знакомы с такими системами в достаточной степени, чтобы давать в отношении них объективные замечания; в некоторых случаях может потребоваться назначение профильного аудитора.

Для обзора данных персонал службы обеспечения качества должен иметь прямой доступ «только для чтения» к данным, хранящимся в компьютеризированной системе.

3.2.2 Обучение

Принципы GLP требуют, чтобы испытательный центр имел квалифицированный и опытный персонал надлежащего уровня, документированные учебные программы как для обучения на рабочем месте, так и при необходимости на внешних учебных курсах. Записи о подобном обучении должны быть сохранены.

Вышеуказанные положения должен также применять весь персонал, использующий компьютеризированные системы.

3.2.3 Помещения и оборудование

Для проведения исследований в соответствии с требованиями Принципов GLP требуется наличие соответствующих помещений и оборудования. Рассматривая компьютеризированные системы, следует принять во внимание ряд конкретных положений.

a) Помещения

Необходимо уделять должное внимание физическому расположению компьютерного аппаратного обеспечения, периферийных компонентов, коммуникационного оборудования и электронных носителей информации. Следует избегать экстремальных температур и влажности, пыли, электромагнитных

помех и близости к кабелям высокого напряжения, кроме случаев, когда оборудование специально предназначено для работы в подобных условиях.

Также необходимо уделять внимание электропитанию компьютерного оборудования и при необходимости резервному копированию или бесперебойному питанию компьютеризированных систем, неисправность которых может повлиять на результаты исследования.

Необходимо иметь соответствующие помещения для безопасного хранения электронных носителей информации.

b) Оборудование

i) Аппаратное и программное обеспечение

Компьютеризированная система определяется как группа аппаратных компонентов и соответствующего программного обеспечения, разработанная и собранная для выполнения определенной функции или группы функций.

К аппаратному обеспечению относятся физические компоненты компьютеризированной системы, состоящие из самого компьютера и периферийных компонентов.

Программное обеспечение представляет собой программу(ы), управляющую(ие) функционированием компьютеризированной системы.

Все Принципы GLP, применяемые к оборудованию, в равной степени применимы и к аппаратному, и к программному обеспечению.

ii) Коммуникации

Коммуникации, относящиеся к компьютеризированным системам, делятся на две основные категории: коммуникации между компьютерами или между компьютерами и периферийными компонентами.

Все коммуникационные линии являются потенциальными источниками ошибок, которые могут привести к потере или повреждению данных. Для обеспечения безопасности и целостности системы должен быть установлен соответствующий контроль процессов разработки, валидации, эксплуатации и технического обслуживания компьютеризированных систем.

3.2.4 Техническое обслуживание и аварийное восстановление

Все компьютеризированные системы следует устанавливать и обслуживать таким образом, чтобы обеспечивать непрерывность работы.

a) Техническое обслуживание

Обязательно наличие документированных процедур, охватывающих как плановое профилактическое обслуживание, так и устранение неисправностей. В этих процедурах должны быть четко определены роль и ответственность вовлеченного в процесс технического обслуживания персонала. В случаях, когда такие операции по сопровождению требуют изменений аппаратного и/или программного обеспечения, может возникнуть необходимость повторной валидации системы. В течение повседневной работы должна записываться информация о любых проблемах и несоответствиях в системе и любые предпринятые действия по исправлению положения.

b) Аварийное восстановление

Должны иметь место процедуры, описывающие меры, которые необходимо предпринять в случае частичного или полного отказа компьютеризированной системы. Меры могут варьироваться от запланированного сокращения аппаратного оборудования до перехода в систему с бумажными носителями информации. Все планы действия в аварийных ситуациях должны быть тщательно документированы, валидированы; кроме того, они должны обеспечивать непрерывную целостность данных и не должны каким-либо образом угрожать исследованию. Персонал, вовлеченный в проведение исследования в соответствии с Принципами GLP, должен быть осведомлен о наличии данных планов действия в аварийных ситуациях.

Процедуры восстановления компьютеризированной системы будут зависеть от критичности системы, поэтому так важно иметь в наличии резервные копии всех программ. Если процедуры восстановления влекут за собой изменения аппаратного или программного обеспечения, может потребоваться повторная валидация системы.

3.2.5 Данные

Принципы GLP определяют первичные данные как оригиналы записей и документации, включая данные, напрямую введенные в компьютер через интерфейс прибора, которые являются результатами оригинальных наблюдений и действий в ходе исследования и необходимы для формирования и оценки отчета о данном исследовании.

Компьютеризированные системы, работающие в соответствии с Принципами GLP, могут быть связаны с первичными данными с использованием различных форм, таких как, например, электронные

носителии информации, распечатки с компьютера или приборов, а также копии микрофильмов/микрофиш. Необходимо, чтобы первичные данные были определены для каждой компьютеризированной системы.

Если компьютеризированные системы используют для сбора, обработки, представления или хранения первичных данных в электронном виде, то конфигурация системы всегда должна обеспечивать сохранение аудиторских данных в полном объеме, чтобы была возможность показать все изменения данных, не скрывая первичных данных. Должна быть возможность связать все изменения данных с лицами, которые внесли эти изменения при помощи своевременной и датированной (электронной) подписи. Причины внесения изменений должны быть указаны.

Если первичные данные хранятся на электронных носителях информации, то необходимо обеспечить выполнение требований по их долгосрочному хранению в зависимости от типа хранимых данных и ожидаемого срока службы компьютеризированных систем. При изменении систем аппаратного и программного обеспечения должны быть предоставлены постоянный доступ к первичным данным и их безопасное хранение для гарантирования целостности данных. Вспомогательная информация, такая как журналы обслуживания оборудования и протоколы калибровки, которая необходима для подтверждения достоверности первичных данных или которая позволяет реконструировать процесс или исследование, должна быть сохранена в архивах.

Процедуры для работы компьютеризированной системы также должны описывать альтернативные процедуры сбора данных, которым необходимо следовать в случае сбоя системы. При таких обстоятельствах любые вручную записанные исходные данные, в дальнейшем вводимые в компьютер, должны быть четко обозначены в качестве таковых и сохранены в качестве исходных записей. Процедуры по резервированию данных, проводимые вручную, должны свести к минимуму риск потери данных и гарантировать сохранение этих альтернативных записей.

Если в случае устаревания системы необходимо перевести электронные первичные данные из одной системы в другую, то данный процесс должен быть документирован надлежащим образом, а целостность данных подтверждена. В случаях, когда подобные миграции данных не осуществимы практически, первичные данные должны быть переданы на другой носитель и утверждены в качестве точной копии до начала удаления оригинальных электронных записей.

3.2.6 Безопасность

Для защиты аппаратного оборудования, программного обеспечения и данных от повреждения, несанкционированного изменения или потери данных должны быть установлены документированные процедуры безопасности.

В данном контексте «безопасность» означает предотвращение несанкционированного доступа или изменений как компьютеризированной системы, так и данных, хранящихся в ней. Следует также принять во внимание вероятность повреждения данных вирусами или другими программами-агентами. Также должны быть приняты меры безопасности, обеспечивающие целостность данных в случае как краткосрочных, так и долгосрочных сбоев системы.

a) Физическая безопасность

Чтобы ограничить доступ к компьютерному и коммуникационному оборудованию, периферийным компонентам и электронным носителям информации только уполномоченным персоналом, необходимо применять физические меры безопасности.

К оборудованию, которое не хранится в специальных «компьютерных помещениях» (например, персональным компьютерам и терминалам), должны применяться, как минимум, стандартные элементы контроля доступа, имеющиеся в испытательном центре.

Однако там, где такое оборудование располагается удаленно (например, портативные компоненты и линии модемной связи), должны быть приняты дополнительные меры.

b) Логическая безопасность

Чтобы предотвратить несанкционированный доступ к компьютеризированной системе, приложениям и данным, необходимо наличие мер логической безопасности для каждой компьютеризированной системы или приложения. Важно обеспечивать использование только утвержденных версий и валидированного программного обеспечения. Логическая безопасность может включать в себя необходимость введения уникального идентификатора пользователя с соответствующим паролем. Любое введение данных или установку программного обеспечения из внешних источников следует контролировать. Эти элементы контроля могут обеспечиваться с помощью программного обеспечения операционной системы компьютера, специальных программ безопасности, встроенных в приложения процедур, или комбинаций всего вышеперечисленного.

c) Целостность данных

Так как поддержание целостности данных является главной целью Принципов GLP, важно, чтобы весь персонал, связанный с компьютеризированной системой, осознавал необходимость вышеизложенных мер безопасности. Администрация испытательного центра должна гарантировать, чтобы персонал был осведомлен о важности обеспечения безопасности данных, доступных процедурах и особенностях системы, которые позволяют предоставить надлежащую безопасность, а также о последствиях нарушения безопасности.

Такие функции системы могут включать плановое наблюдение за доступом к системе, внедрение программ верификации файлов и отчетов об исключениях и/или трендах.

d) Резервное копирование

Резервное копирование программного обеспечения и данных является стандартной практикой при работе с компьютеризированной системой, которая позволяет восстановить систему после любых неполадок (например, повреждения диска), ставящих под угрозу целостность системы. В данном случае подразумевается возможность превращения резервной копии в первичные данные, после чего они должны рассматриваться в качестве таковых.

3.2.7 Валидация компьютеризированных систем

Компьютеризированные системы должны быть пригодны для предусмотренного назначения. Должны быть рассмотрены следующие аспекты:

a) приемочные испытания

Компьютеризированные системы должны быть спроектированы так, чтобы удовлетворять Принципам GLP. Они должны быть установлены согласно предварительно разработанному плану. При этом необходимо наличие соответствующей документации, подтверждающей, что каждая система была разработана под соответствующим контролем и (желательно) в соответствии с общепризнанными стандартами качества и техническими стандартами (например, ГОСТ Р ИСО 9001:2008 (ISO 9001)). Кроме того, должны быть предоставлены доказательства того, что система была надлежащим образом протестирована испытательным центром на соответствие критериям приемки до введения в повседневное использование.

Процедура официального приемочного испытания требует проведения испытаний в соответствии с заранее установленным планом и сохранения документированного свидетельства, содержащего следующую информацию: процедуры испытания, данные проведенного испытания, результаты испытаний, официальную сводку об испытании, записи об официальной приемке результатов испытания.

Вполне вероятно, что бóльшая часть документации, относящейся к установленным производителем системам и созданной в процессе разработки систем, хранится на сайте производителя. В этом случае данные официальной оценки и/или аудита производителя должны быть в наличии в испытательном центре;

b) ретроспективная оценка

Имеются системы, для которых необходимость соблюдения Принципов GLP не была предусмотрена или указана. В таких случаях необходимо наличие документального обоснования использования данных систем, которое должно включать в себя ретроспективную оценку, используемую для определения пригодности системы.

Ретроспективная оценка начинается со сбора всех исторических записей, связанных с компьютеризированной системой. Затем данные записи рассматриваются, после чего составляется письменная сводка. В данной сводке ретроспективной оценки необходимо указывать, что доказательства валидации доступны, а также какие шаги следует предпринимать в будущем для обеспечения валидации компьютеризированной системы;

c) контроль изменений

Контроль изменений означает официальное утверждение и документирование любого изменения компьютеризированной системы в течение срока ее эксплуатации. Контроль изменений необходим в случаях, когда изменения могут повлиять на статус валидации компьютеризированной системы. Процедуры контроля изменений должны вступать в силу сразу после подтверждения готовности к эксплуатации компьютеризированной системы.

В процедуре должен быть описан метод оценки, призванный определять объем повторного испытания, необходимого для поддержания системы в валидированном состоянии. В рамках процедур контроля изменений должны быть определены лица, ответственные за определение необходимости и одобрение контроля изменений.

Независимо от источника происхождения изменения (поставленная вендором система или система собственной разработки) соответствующая информация должна быть представлена как часть процесса контроля изменений. Процедуры контроля изменений должны гарантировать целостность данных;

d) механизм поддержки

В целях обеспечения соответствия компьютеризированной системы предусмотренному назначению должны быть созданы механизмы поддержки, обеспечивающие корректное функционирование и использование системы. Они могут включать в себя систему управления, обучение, обслуживание, техническую поддержку, аудит и/или оценку эксплуатационных показателей. Оценка эксплуатационных показателей означает номинальный просмотр системы через определенные промежутки времени с целью подтверждения соответствия установленным критериям функционирования, например надежности, чувствительности, производственной мощности.

3.2.8 Документирование

Перечисленные ниже пункты представляют собой руководство по подбору минимальной документации для разработки, валидации, эксплуатации и техническому обслуживанию компьютеризированных систем.

a) Порядок действий

Необходимо наличие письменно зафиксированных принципов административного управления, описывающих помимо прочего процесс приобретения, требования, проектирование, валидацию, испытание, установку, эксплуатацию, техническое обслуживание, подбор персонала, контроль, аудит, мониторинг и изъятие из обращения компьютеризированных систем.

b) Описание приложения (прикладного программного обеспечения)

Каждое приложение должно сопровождаться документацией, в которой полностью описывается:

- наименование приложения или идентификационного кода и подробное и четкое описание целей приложения;
- аппаратное обеспечение (с номерами моделей), на которое установлено приложение;
- программное обеспечение операционной и другой системы (например, инструментов), используемое в сочетании с приложением;
- используемый(ые) программируемый(ые) язык(и) приложения и/или инструментов базы данных;
- основные функции, выполняемые приложением;
- обзор типов и потоков данных/дизайна баз данных, связанных с приложением;
- структуры файлов, сообщения об ошибках и авариях, а также алгоритмы, связанные с приложением;
- компоненты прикладного программного обеспечения с указанием номеров версий;
- конфигурация и коммуникационные связи между модулями приложения, а также оборудованием и другими системами.

c) Исходный код

Некоторые страны — члены ОЭСР требуют, чтобы исходный код прикладного программного обеспечения был доступен испытательному центру (либо должна быть предоставлена возможность извлечь его).

d) Стандартные операционные процедуры (СОП)

Бóльшая часть документации, охватывающей использование компьютеризированных систем, должна быть представлена в форме СОП. Данные СОП должны охватывать следующие процедуры, но не ограничиваться ими:

- процедуры по работе с компьютеризированными системами (аппаратные средства/программное обеспечение) и обязанности/ответственность вовлеченного персонала;
- процедуры по обеспечению мер безопасности, используемых для обнаружения и предотвращения несанкционированного доступа к программе и внесения в нее изменений;
- процедуры по внесению изменений в программу, их авторизации и записи изменений;
- процедуры по внесению изменений в оборудование (аппаратные средства/программное обеспечение) и их авторизации, в том числе, в случае необходимости, проведение испытаний перед использованием оборудования;
- процедуры по проведению периодического испытания надлежащего функционирования всей системы или ее составных частей и записи данных испытаний;
- процедуры обслуживания компьютеризированных систем и любого сопутствующего оборудования;

- процедуры разработки программного обеспечения и приемочных испытаний, а также записи всех приемочных испытаний;

- процедуры по резервному копированию всех хранимых данных, а также планы действия в случае поломки;

- процедуры архивирования и извлечения всех документов, программного обеспечения и компьютерных данных;

- процедуры мониторинга и аудита компьютеризированных систем.

3.2.9 Архивы

Принципы GLP по архивированию данных следует применять последовательно ко всем типам данных. Поэтому очень важно, чтобы электронные данные хранились на том же уровне контроля доступа, индексирования и соответствующего извлечения, как и другие типы данных.

Если электронные данные о нескольких исследованиях хранятся на одном носителе информации (например, диске или магнитной ленте), требуется создание подробного указателя. Он может быть необходим для обеспечения испытательных центров средствами контроля окружающей среды, чтобы гарантировать целостность хранимых электронных данных. Если существует необходимость в создании дополнительных архивных помещений, то администрация испытательного центра должна обеспечивать, чтобы персонал, ответственный за управление архивами, был идентифицирован и чтобы доступ к архиву был возможен только уполномоченному персоналу. Также необходимо будет внедрить процедуры, гарантирующие, что целостность хранящихся в электронном виде в течение длительного времени данных не будет нарушена.

Необходимо создание процедур, обеспечивающих непрерывную считываемость данных в случаях, когда предполагается возникновение проблем с долгосрочным доступом к данным или возникает необходимость изъятия компьютеризированных систем из употребления. Такими процедурами могут быть, например, производство твердых копий в форме распечатки с принтера или перенос данных в другую систему.

Хранящиеся в электронном виде данные не следует уничтожать без разрешения администрации испытательного центра и соответствующего документирования. Другие данные, хранящиеся в поддержку компьютеризированных систем, такие как исходный код и записи о разработке, валидации, эксплуатации, обслуживании и мониторинге, следует хранить, по крайней мере, в течение того же срока, как и записи об исследовании, связанные с данными системами.

Библиография

[1] OECD series on Principles of Good Laboratory Practice and Compliance Monitoring — No 10 — GLP consensus document. The application of the principles of GLP to computerized systems:1995 (Консенсусный документ по GLP. Применение Принципов надлежащей лабораторной практики к компьютеризированным системам:1995, № 10 из серии документов Организации экономического сотрудничества и развития (ОЭСР) о Принципах GLP и мониторинге соответствия)

УДК 502.3/504.03:615.9/615.07:004.9:006.354

МКС 03.120.10
19.020
35.100.70

Ключевые слова: принципы надлежащей лабораторной практики, GLP, обеспечение качества испытаний, компьютеризированные системы, лабораторная информационная менеджмент-система (ЛИМС), валидация, целостность данных

Редактор *Л.И. Нахимова*
Технический редактор *В.Н. Прусакова*
Корректор *О.В. Лазарева*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 25.09.2018. Подписано в печать 01.10.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,35.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru