ГОСТ Р 57680-2017

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Производство лекарственных средств

РУКОВОДСТВО ПО ИСПОЛЬЗОВАНИЮ КОМПЬЮТЕРИЗОВАННЫХ СИСТЕМ В СИСТЕМАХ КАЧЕСТВА *GxP*

Manufacturing of medicinal product. Guidance for using computerized systems in quality systems regulated *GxP*

ОКС 13.060.70

Дата введения 2018-08-01

Предисловие

1 РАЗРАБОТАН Государственным образовательным учреждением высшего образования Первым Московским государственным медицинским университетом имени И.М.Сеченова Министерства здравоохранения Российской Федерации (Первым МГМУ имени И.М.Сеченова)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 458 "Разработка, производство и контроль качества лекарственных средств"

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 сентября 2017 г. N 1166-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного документа "Руководство PIC/S PI 011-3* "Использование компьютеризованных систем в системах качества "*GxP*" ("Good practices for computerized systems in regulated "*GxP*" environments", NEQ) Конвенции по фармацевтическим инспекторатам/Схемы взаимодействия фармацевтических инспекторатов (Pharmaceutical inspection convention/pharmaceutical inspection cooperation scheme; PIC/PIC/S)

_____

* Доступ к международным и зарубежным документам, упомянутым в тексте, можно получить, обратившись в Службу поддержки пользователей. - Примечание изготовителя базы данных.

Наименование настоящего стандарта изменено относительно наименования указанного международного документа для приведения в соответствие с ГОСТ Р 1.5-2012 (пункт 3.5)

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Июль 2019 г.

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. N 162-ФЗ "О стандартизации в Российской Федерации". *Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе "Национальные стандарты", а официальный текст изменений и поправок - в ежемесячном информационном указателе "Национальные стандарты". В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя "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 (www.gost.ru)*

Введение

Информационные технологии развиваются со значительной скоростью, и организации, работающие по надлежащим практикам, должны обеспечить разработку систем и программного обеспечения в условиях наилучших инженерных практик и соответствующих аспектов обеспечения качества.

Настоящий стандарт представляет собой логическое объяснение основных требований к внедрению, валидации и эксплуатации компьютеризованных систем (далее - КС) и может быть использован для определения критериев соответствия установленных требований к КС в надлежащих практиках. Он не является обязательным для применения, однако организации могут применять его рекомендации.

Настоящий стандарт содержит детальное описание лучших отраслевых практик в отношении применения КС, поддерживая развитие новых технологий и технологические инновации.

Настоящий стандарт разработан на основе Руководства PIC/S PI 011-3 по использованию компьютеризованных систем в системах качества *GxP* (PIC/S PI 011-3 "Good practices for computerized systems in regulated "*GxP*" environments") Конвенции по фармацевтическим инспекторатам/Схемы взаимодействия фармацевтических инспекторатов (Pharmaceutical inspection convention/Pharmaceutical inspection cooperation scheme; PIC/PIC/S), в разработке которого приняли участие международные регуляторные органы.

1 Область применения

Область применения настоящего стандарта распространяется на использование КС в организациях, осуществляющих работы в сфере обращения лекарственных средств в соответствии с правилами надлежащей производственной практики, надлежащей дистрибьюторской практики. Также он может применяться организациями, работающими в соответствии с надлежащей лабораторной практикой.

Организации сами определяют пригодное для них программное приложение, подразделения, в которых оно внедряется, и соответствующие результаты его работы. В настоящем стандарте описаны подходы и виды контроля (параметры), которые могут быть использованы для обеспечения соответствия данных работ требованиям надлежащих практик.

Также настоящий стандарт описывает основные этапы и документацию в отношении внедрения и валидации КС в организации, включая различные подходы к разным типам систем и различные виды валидации.

Учитывая итеративный характер КС, в настоящем стандарте также представлены рекомендации для поставщиков и разработчиков приложений и автоматизированных систем, поставляемых в организации, работающие в условиях надлежащих практик.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

ГОСТ Р ИСО 9004 Менеджмент для достижения устойчивого успеха организации. Подход на основе менеджмента качества

ГОСТ Р ИСО 10005 Менеджмент организации. Руководящие указания по планированию качества

ГОСТ Р ИСО 10007 Менеджмент организации. Руководящие указания по управлению конфигурацией

ГОСТ Р ИСО/МЭК 12207 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств

ГОСТ Р ИСО/МЭК 25010 Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов

ГОСТ Р ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

Примечание - При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю "Национальные стандарты", который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя "Национальные стандарты" за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по [1], [2], руководству GAMP, техническим руководствам по КС, а также следующие термины с соответствующими определениями:

3.1 **автоматизированные системы** (Automated System): Широкий спектр систем, включая автоматизированное производственное оборудование, контрольные системы, автоматизированные лабораторные системы, производственные исполнительные системы и компьютеры, управляющие лабораторными или производственными базами данных.

Примечание - Автоматизированные системы состоят из оборудования, компонентов программного обеспечения (ПО) и компьютерной сети, включая контролируемые функции и связанную документацию. Автоматизированные системы иногда также называют КС. В настоящем стандарте данные термины являются синонимами.

3 . 2 **безопасность** (Security): Защита компьютерного оборудования и программных приложений от случайного или преднамеренного доступа, применения, изменения, разрушения или раскрытия.

Примечание - Безопасность также касается персонала, данных, коммуникаций и физической защиты компьютерной инфраструктуры.

3 . 3 **валидация компьютеризированных систем** (Validation of Computerised Systems): Документально оформленные действия, дающие высокую степень уверенности в том, что система соответствует заданным требованиям и ее использование будет постоянно приводить к результатам, соответствующим заранее установленным критериям приемлемости.

3.4 **владелец процесса** (Process owner): Лицо, ответственное за рабочий процесс.

3 . 5 **владелец системы** (System owner): Лицо, ответственное за доступность и техническое обслуживание КС и безопасность данных, находящихся в этой системе.

3 . 6 **встроенная система** (Embedded System): Система, обычно микропроцесс или программируемый контроллер, единственное назначение которой контролировать определенный элемент автоматизированного оборудования.

Примечание - Она не является отдельной компьютерной системой.

3.7 **встроенное программное обеспечение** (Firmware): ПО, записанное в компьютерное оборудование без возможности удаления, например EPROM.

3.8 **гибридные системы** (Hybrid Systems): Гибридная система - система, в которой используется комбинация ручного управления и автоматизированных функций.

3.9 **жизненный цикл** (Life Cycle Concept): Все стадии существования КС от формирования первоначальных требований до прекращения эксплуатации, включая проектирование, определение технических требований, программирование, тестирование, установку, эксплуатацию и обслуживание.

3 . 1 0 **интеграционное тестирование** (Integration testing): Поэтапное проведение тестирования элементов ПО, элементов компьютерного оборудования или и того, и другого, продолжающееся до полной интеграции всей системы.

3.11 **интерфейс** (Interface): Общая граница двух отдельно существующих составных частей для взаимодействия или обмена информацией с другим элементом системы.

3 . 1 2 **информационно-технологическая инфраструктура** (IT Infrastructure): Компьютерное оборудование и ПО, такое как сетевое ПО и операционные системы, которые позволяют их применить для выполнения определенных функций.

3.13 **инфраструктура открытых ключей;** ИОК (Public Key Infrastructure (PKI)): ИОК предоставляет структуру для безопасного обмена информацией путем использования криптографической системы с открытым ключом и электронных сертификатов.

Примечание - ИОК может состоять из многочисленных доменов, но наиболее важны два типа:

- частную ИОК используют компания для целей своего бизнеса и связанные с ней стороны (например, потребители, поставщики);

- публичную ИОК (привлекают доверенную третью сторону) развертывают на открытых системах, таких как Интернет, что обеспечивает безопасность обмена информацией между ранее не связанными сторонами.

3.14 **исполнительная программа** (Executive Program): Программа, представляющая собой часть операционной системы, которая контролирует выполнение других программ и регулирует поток работ в системе обработки данных.

3.15 **исходный код** (Source Code): Оригинальная компьютерная программа, изложенная в читаемой форме (на языке программирования), которая может быть переведена в машинный код до ее выполнения компьютером.

3.16 **компьютеризированная система** (Computerised System): Система, подразумевающая: процесс или операцию, объединенную в одно целое с компьютерной системой, включающих ввод данных, их электронную обработку и выдачу информации, используемой для документального оформления и (или) для автоматического управления; компьютерную систему и контролируемые функции, которыми она управляет.

Примечание - Приводимое определение достаточно ограничено. В эту систему входят также все внешние эффекты, которые взаимодействуют с системой в ее операционном окружении. Это могут быть мониторинговые и сетевые связи (в/из других систем или оборудования), ручные (ввод с клавиатуры), связи с различными средами, ручными процедурами и автоматикой. Данный термин также охватывает автоматизированное оборудование и системы (см. также термин "автоматизированные системы"). В настоящем стандарте они являются аналогами.

3.17 **компьютеризированная система, изготовленная по индивидуальному заказу** (Bespoke): Индивидуально спроектированная КС для обеспечения конкретного рабочего процесса.

3.18 **компьютерная сеть** (Network): Соединенная или взаимосвязанная группа узлов; объединенные коммуникационные мощности.

3.19 **локальная сеть** (LAN): Широкополосная компьютерная сеть (обеспечивающая высокую скорость передачи данных), функционирующая на небольшом пространстве, например офис или группа офисов.

3.20 **компьютерная система** (Computer System): Компоненты компьютерного оборудования, собранные для функционирования вместе с приложениями, которые коллективно спроектированы для выполнения определенной функции или группы функций (см. рисунок 1).

3.21 **компьютерное оборудование** (Computer Hardware): Различные виды оборудования в компьютерной системе, включая центральный процессор, принтер, модем, монитор и другие присоединенные устройства (см. рисунок 1).

3.22 **контроль изменений** (Change Control): Документально оформленный порядок рассмотрения уполномоченными представителями различной специализации предложенных или фактически внесенных изменений, которые могут повлиять на валидированное состояние помещений, оборудования, систем или процессов.

Примечание - Цель такого контроля - определить необходимость проведения мероприятий, которые должны обеспечить и документально удостоверить поддержание системы в валидированном состоянии.

3.23 **конфигурация** (Configuration): Задокументированные физические и функциональные характеристики определенного элемента, системы, например приложения, оборудования, встроенное программное обеспечение и операционная система.

Примечание - Изменение превращает одну конфигурацию в другую.

3.24 **конфигурируемые серийные программы** (Commercial off-the-shelf; COTS): Коммерческие серийные программы, которые могут быть сконфигурированы для определенных приложений пользователя путем "заполнения бланков", без изменения базовой программы.

3.25 **незапланированные (экстренные) изменения** Unplanned (Emergency) Change: Непредвиденные (экстренные) изменения в валидированной системе, требующие быстрого внедрения (хотфиксы).

3.26 **операционная система** (Operating System): Набор программ, предоставляемых вместе с компьютером в качестве интерфейса между компьютерным оборудованием и программами-приложениями.

3.27 **операционное окружение** (Operating Environment): Условия и деятельность, взаимодействующие непосредственно или косвенно с анализируемой системой, контроль которых может влиять на валидированное состояние системы.

3.28 **организация** (Regulated User): Регулируемая надлежащей практикой структура, ответственная за эксплуатацию КС и приложений, файлов и содержащихся в них данных (см. также термин "пользователь").

3.29 **отдельная система** (Standalone System): Автономная компьютерная система, которая позволяет проводить обработку данных, предоставляет функции управления и мониторинга, однако не совмещенная с автоматизированным оборудованием. Это отличает ее от встроенной системы, чьим единственным предназначением является управление конкретным экземпляром автоматизированного оборудования.

3.30 **отладка** (Debugging): Процесс нахождения, анализа и исправления предполагаемых ошибок (в приложении).

3.31 **ошибка в программе или системе** (Bug): Ошибка в программе или системе, из-за которой программа выдает неожиданное поведение и, как следствие, результат.

3.32 **первичные/исходные данные** (Raw Data): Любые таблицы, записи, заметки или их точные копии, представляющие собой результаты исходных наблюдений и действий и необходимые для восстановления и оценки рабочего проекта, процесса или отчета исследования и т.п.

Примечание - Первичные данные могут существовать в бумажном или электронном виде, их вид должен быть определен и описан в основных процедурах.

3.33 **повторная валидация** (Revalidation): Повторение процесса валидации или его части.

3.34 **пользователь** (User): Компания или группа лиц, ответственная за функционирование системы.

Примечание - См. также термин "организация". В контексте настоящего стандарта - синоним термина "потребитель".

3.35 **приложение** (Application): Программное обеспечение, установленное на определенной платформе или компьютерном оборудовании и предоставляющее специальные функциональные возможности.

3.36 **проверка цикла/тестирование цикла** (Loop Testing): Проверка установленной комбинации элементов, характеризующих каждый тип входа/выхода цикла.

3.37 **проектная спецификация оборудования** (Hardware Design Specification): Описание компьютерного оборудования, в котором будет использоваться ПО, и его соединение с другой системой или оборудованием.

3.38 **ранее установленные системы** (Legacy Computerised Systems): Системы, которые созданы достаточно давно и используются в течение длительного промежутка времени.

Примечание - По ряду причин для подобных систем может отсутствовать GMP-документация и записи, относящиеся к этапам разработки системы и ее ввода в эксплуатацию. Кроме того, могут отсутствовать записи относительно формализованного подхода к валидации системы, что связано с ее возрастом.

3.39 **серийное программное обеспечение** (Commercial of the shelf software): Коммерчески доступное ПО, пригодность которого для использования продемонстрирована большим количеством пользователей.

3.40 **системное программное обеспечение** (System Software): ПО, спроектированное для облегчения управления и обслуживания компьютерной системы и связанных с нею программ, например операционных систем, ассемблеров, вспомогательных программ, сетевого ПО и исполняющих программ.

Примечание - Системное ПО, как правило, не зависит от конкретного применения системы.

3.41 **служебное программное обеспечение** (Utility Software): Компьютерные программы или последовательности, предназначенные для выполнения общих вспомогательных функций, необходимых для иного ПО, операционной системы или пользователя системы.

3.42 **специализированное приложение** (Application-Specific Software): ПО, разработанное или адаптированное для определенных требований приложения.

3.43 **спецификации приемочных испытаний системы** (System Acceptance Test Specification [3]): Описание испытаний, проведение которых является необходимым для приемки системы пользователем.

Примечания

1 Обычно испытания охватывают функциональность системы; производительность системы, критические параметры, операционные процедуры.

Испытания должны подтвердить, что продукт функционирует согласно функциональным спецификациям и соответствует требованиям пользователя, описанным в спецификациях требований пользователя.

2 Испытания, как правило, включают в себя тестирование в предельных условиях, в аварийном состоянии и граничные испытания.

Спецификации приемочных испытаний системы являются контрактным документом и должны быть одобрены всеми сторонами (поставщиком, разработчиком, интегратором и конечным пользователем).

3.44 **спецификации системы** (System Specifications): Описание выполнения системой функциональных требований.

3.45 **спецификация на приемочные испытания оборудования** (Hardware Acceptance Test Specification): Требования по проверке всех ключевых аспектов установки компьютерного оборудования с целью соблюдения соответствующих требований и одобренных характеристик при проектировании и учет основных рекомендаций организации.

3.46 **структурная верификация** (Structural Verification): Действия, направленные на получение документального свидетельства того, что ПО имеет надлежащую структурную целостность.

3.47 **структурная целостность** (программного обеспечения) [Structural Integrity (Software)]: Свойства ПО, отражающие степень, в которой исходный код соответствует специфицированным требованиям и современным практикам разработки ПО.

3.48 **структурное тестирование** (Structural Testing): Изучение внутренней структуры исходного кода, включающее в себя низкоуровневый и высокоуровневый анализ кода, анализ пути, аудит методов программирования и использованных стандартов, инспектирование на наличие внешнего "неиспользуемого кода", анализ граничных значений и прочие методы.

Примечание - Для проведения структурного тестирования требуются конкретные навыки программирования и знание компьютерных технологий.

3.49 **управление конфигурацией** (Configuration Management): Процесс идентификации и определения элементов системы, контроля запуска и изменения этих элементов на протяжении жизненного цикла системы, ведение записей и отчетов о статусе конфигурации и запросов на изменения, а также подтверждение полноты и корректности элементов конфигурации.

3.50 **усиленная электронная подпись** (Advanced Electronic Signature): Электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ, обнаружить факт внесения изменений в электронный документ после его подписания;
- создана с использованием средств электронной подписи.

3.51 **функциональное тестирование** (Functional Testing): Процесс подтверждения того, что приложение, система или элемент системы выполняют свои назначенные функции.

3.52 **функциональные спецификации** (Functional Specifications): Требования, которые описывают, каким образом КС должна удовлетворять функциональные требования связанной с компьютером системы.

3.53 **функциональные требования** (Functional Requirements): Требования, описывающие функции, которые должна выполнять связанная с компьютером система.

3.54 **электронная подпись** (Electronic Signature): Электронная, цифровая подпись, эквивалентная обычной подписи.

3.54.1 Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и использована для определения лица, подписывающего информацию [2].

3.54.2 Электронное средство, которым можно заменить рукописную подпись или инициалы для целей согласования, разрешения или подтверждения ввода определенных даннах* (PIC/S).

_____

* Текст документа соответствует оригиналу. - Примечание изготовителя базы данных.

3.54.3 Компиляция данных из символов или серий символов, выполняемая, принимаемая или утверждаемая любым лицом в качестве легально обязывающего эквивалента его рукописной подписи.

3.54.4 Данные в электронной форме, которые присоединены или логически связаны с другими электронными данными и использованы в качестве идентификации лица (EU).

4 Общие положения

4.1 Структура и функции компьютеризованных систем

4.1.1 КС состоит из компьютерной системы и контролируемой функции или процесса. Компьютерная система представляет собой всю совокупность аппаратного и программного обеспечения (контролирующего аппаратное обеспечение), а также встроенного ПО и установленных устройств. Контролируемая функция может представлять собой оборудование (например, автоматизированное производственное оборудование, лабораторные или технологические контрольно-измерительные приборы), которым необходимо управлять, и алгоритмы действий, определяющих его работу. В качестве контролируемой функции также может выступать операция, для выполнения которой не требуется другого оборудования, за исключением аппаратного обеспечения компьютера. Интерфейсы и сетевые функции [через локальную вычислительную сеть (ЛВС, LAN) и глобальную вычислительную сеть (ГВС, WAN)] также являются особенностями КС и операционного окружения, потенциально связывающими воедино множество компьютеров и приложений (см. рисунок 1). Информационно-технологическая инфраструктура организации, функциональность и взаимодействие с прочими системами должны быть четко определены и подлежат контролю в соответствии с действующими правилами надлежащей производственной практики (приложение 11) [1].

Рисунок 1 - Схема взаимодействия различных компонентов КС в ее операционном окружении

4.1.2 В упрощенном виде КС по их назначению можно разделить на три категории: системы контроля процессов, системы обработки данных [включая сбор (захват) данных] и системы записи/хранения данных. Между указанными системами могут встраиваться связующие элементы (интерфейсы). Гарантия целостности[1)] как процессов, выполняемых в контролируемой компьютерной системе, так и процессов, контролируемых КС в рамках ее операционной среды, должна быть подтверждена посредством валидации.

[1)] Состояние ПО и данных, характеризующееся отсутствием изменений преднамеренного или случайного характера (ГОСТ Р 8.654-2015 Государственная система обеспечения единства измерений. Требования к программному обеспечению средств измерений. Основные положения).

4.1.3 В организациях используется большое количество различных КС, начиная от небольших несетевых и заканчивая сложными и интегрированными. Часть из них (существенная доля производственного, лабораторного и клинического оборудования) имеет встроенное ПО, серийное ПО, стандартные операционные системы. Также в КС могут использоваться специализированные приложения. Организация должна вести перечень (реестр) всех применяемых КС с указанием владельца, поставщика (разработчика), функциональности, связей и валидационного статуса. Также в наличии должен быть основной валидационный план и порядок проведения валидации КС .

4.1.4 К критическим КС с точки зрения надлежащих практик *GxP* относятся системы, которые могут оказать негативное влияние на качество продукции и безопасность пациентов или непосредственно (например, контрольные системы) нарушить целостность связанной с продукцией информации (например, системы обработки данных/информационные системы, задействованные в кодировании и маркировке, рандомизации, распределении, отзыве продукции с рынка, клинических измерениях, записях пациентов, источниках дотаций, лабораторных данных и т.д.). Данные примеры не являются исчерпывающими.

4.2 Управление рисками

4.2.1 Управление рисками следует применять в течение всего жизненного цикла КС (то есть на всех стадиях существования КС - от формирования первоначальных требований до прекращения эксплуатации, включая проектирование, определение технических требований, программирование, тестирование, установку, эксплуатацию и обслуживание) в целях обеспечения безопасности пациентов, целостности данных и качества продукции.

4.2.2 Оценку потенциальных рисков для качества продукта/материала или целостности данных либо обеспечения качества проводят для каждого элемента КС или их совокупности (см. рисунок 1) на предмет оценки пригодности системы для ее предназначения. Все работы по оценке рисков регистрируют.

4.2.3 В рамках системы управления рисками решения по объему валидационных испытаний и проведению контроля целостности данных должны быть обоснованными, документально оформленными согласно оценке рисков КС и доступными для предоставления лицам, осуществляющим проверку, по их требованию.

4.3 Персонал

4.3.1 Организация должна иметь достаточное количество персонала, имеющего необходимые квалификацию и опыт работы выполнения в соответствии с установленными требованиями задач по планированию, внедрению, эксплуатации, поддержке пользователей приложений, а также для проведения периодических проверок КС.

4.3.2 Должностные обязанности должны быть четко и ясно изложены в письменном виде в понятной для всех сотрудников организации форме. Тот факт, что КС могут брать на себя функции принятия решений, не отменяет юридически установленной ответственности лиц, занимающих ключевые позиции в организации.

4.3.3 Должностные обязанности по управлению всеми информационными и коммуникационными технологиями, КС и проектами (начиная с простых устройств ввода-вывода и программируемых логических контроллеров и заканчивая интегральным администрированием информационных систем или систем бизнес-управления) должны быть четко определены. Данные обязанности должны включать в себя разработку и управление политикой в отношении закупки информационных продуктов, их внедрение, ввод в эксплуатацию и обслуживание, а также разработку и внедрение формальных периодических проверок, оценок и сервисного обслуживания каждой системы, разработку и ведение соответствующей документации и записей этого вида деятельности.

4.3.4 При разработке процедур и документации подразделения по управлению и администрированию информационными технологиями рекомендуется учитывать положения ГОСТ Р ИСО/МЭК 27002.

4.3.5 Необходимо поддерживать тесное сотрудничество между всеми заинтересованными ответственными лицами, вовлеченными в данный процесс, такими как владелец процесса, владелец системы, уполномоченные лица и технический персонал.

4.3.6 До начала перевода процесса с ручного управления на автоматическое (или перед внедрением новой автоматизированной операции) следует осуществить оценку рисков данного шага в отношении безопасности и возможного влияния на качество продукции, например возможность снижения качества и безопасности продукции как результат меньшего участия персонала в процессе. По результатам оценки может потребоваться включение мер по снижению рисков при выполнении такого перевода.

4.3.7 Организация должна обеспечить соответствующее обучение всех сотрудников, в работе которых использованы КС, и их ознакомление с руководствами пользователей этих систем. Данное требование распространяется также на разработчиков систем, сотрудников, выполняющих техническое обслуживание и ремонт, а также лиц, работа которых может повлиять на документированные возможности функционирования системы.

4.3.8 Помимо основного обучения в области КС вновь принятый на работу персонал должен также проходить первичное обучение для выполнения задач, непосредственно выполняемых ими. Организация также должна проводить последующее непрерывное обучение персонала, периодически оценивая его эффективность (путем тестирования).

4.3.9 При обучении должны быть подробно объяснены и обсуждаться концепции *GxP* и жизненного цикла КС, а также предприняты все меры для понимания и применения персоналом этих концепций. Организация обязана хранить документацию о проведении обучения как часть документации жизненного цикла системы (записи об обучении следует хранить в соответствии с процедурами пользователя).

4.4 Поставщики и провайдеры услуг

4.4.1 В том случае если для поставки, установки, настройки, задания конфигурации, интегрирования, валидации, технического обслуживания (в том числе через удаленный доступ), модификации или поддержания КС, оказания связанных с ними услуг или обработки данных привлекаются третьи лица (в частности, поставщики, провайдеры услуг), то производитель и указанные третьи лица заключают договоры. Заключение таких договоров позволяет устанавливать ответственность третьих лиц за надлежащее исполнение своих обязанностей.

4.4.2 Компетентность и надежность поставщиков являются ключевыми условиями выбора поставщика программного продукта или услуг. Выбор КС и ее поставщика должен основываться на предварительно разработанной спецификации требований пользователя, соответствующим образом задокументированной оценки поставщика и оценки рисков для различных опций системы. Информация для этой оценки может быть получена по результатам аудита поставщика и исследования использования различных версий продукта, по данным сообщества и литературы. Для получения гарантий надежности продукта организация оценивает применяемые поставщиком подходы к обеспечению качества при проектировании, разработке, поставке и техническом обслуживании КС. Необходимость аудита поставщика должна быть основана на оценке рисков[1)]. Решение о покупке должно быть основано на задокументированных результатах приемочного тестирования.

---

1) Аудиты, проводимые организацией или 3-й стороной, вместе с маркетинговым анализом могут помочь при оценке надежности и структурной целостности сложных настраиваемых коммерческих систем. При аудитах проверяют систему менеджмента качества и часть, касающуюся закупаемого продукта.

4.4.3 Порядок оценки поставщиков должен быть оформлен документально; работы по оценке поставщиков регистрируют. Для оценки степени надежности поставляемого продукта могут быть использованы данные о деловой репутации поставщиков и провайдеров и опыт предыдущей работы с ними.

4.4.4 Требуемый уровень гарантии структурной целостности, функциональной надежности и постоянной поддержки ПО и компьютерного оборудования, представляющих критические характеристики для КС, может обеспечить соответствие системы менеджмента поставщика общепринятому стандарту. Графики проведения оценки и область сертификации должны соответствовать характеру поставляемого продукта.

4.4.5 При использовании сертификатов соответствия системы менеджмента качества, выданных сертифицирующим органом, например по схеме TickIT, следует удостовериться в том, что область аудита и графики проверки, используемые сторонними сертифицированными аудиторами, включали инженерные стандарты качества, действующие практики, проверку наличия всех контролей и записей, в том числе в отношении несоответствующего требованиям продукта (претензии от пользователей), корректирующих действий, контроля изменений именно поставляемого продукта и его версий. Такой подход может быть использован для формулировки критериев отбора поставщиков.

4.4.6 Для критических КС проверки наличия признанной сертификации системы менеджмента поставщика, как правило, недостаточно (сертификация может быть несоответствующей или неподходящей). В подобных случаях организации следует использовать дополнительные способы оценки пригодности системы и ее поставщика, используя заранее установленные требования, спецификации и ожидаемые риски. Для этих целей можно использовать опросные листы поставщиков, аудиты (в том числе совместные) поставщиков, а также взаимодействие с пользователями и отраслевыми фокус-группами. Как правило, для КС с высоким риском проводят аудит поставщика[1)].

[1)] Руководство GAMP и PDA содержат подробные рекомендации по видам и процедурам аудита поставщиков критических КС.

4.4.7 При привлечении поставщиков к оценке и валидации КС организацией должна быть проведена оценка критических аспектов поставщика, включая его квалификацию и качество выполняемых работ. Принципы, изложенные в руководстве надлежащей автоматизированной производственной практики (GAMP) [4], применимы и для сложных проектов и оборудования с использованием работ по контракту.

4.4.8 Документация, прилагаемая к коммерчески выпускаемым готовым для использования программным продуктам, должна быть рассмотрена уполномоченными работниками производителя на предмет соответствия его требованиям.

4.4.9 Информация о системе менеджмента качества и оценках поставщиков или разработчиков ПО и установленных КС должна быть доступна для предоставления лицам, осуществляющим проверку, по их требованию.

4.5 Документация

4.5.1 В организации должна быть в наличии полная и актуализированная регламентирующая документация по КС и записи и/или отчеты, охватывающие все аспекты проектирования, внедрения и валидации КС.

Для критических КС должны быть в наличии подробное текущее описание физических и логических взаимосвязей, потоков данных и интерфейсов с другими системами или процессами, требуемые ресурсы всего компьютерного оборудования и ПО, доступные меры безопасности, а в документации приведено детализированное описание системы, в том числе ее разработка и условия обслуживания[2)]. В документации может присутствовать ссылка на спецификации требований пользователя или иные документы, описывающие жизненный цикл системы, а также четкое описание того, что система должна или не должна делать. Такая документация должна быть в наличии как для работающих, так и для разрабатываемых систем.

_____

[2)] В качестве подобной документации также могут выступать утвержденные взаимосвязанные записи о жизненном цикле системы. Для крупных комплексных систем информация о разработке и обслуживании может быть приведена в разных документах, на которые должны присутствовать ссылки в общем документе, описывающем систему.

4.5.2 Порядок выполнения и регистрации данных на основных этапах жизненного цикла ПО, связанный с квалификациями и тестированием, должен быть установлен в подробных процедурах или планах качества.

4.5.3 Организация должна разработать и применять политику и процедуры, касающиеся спецификаций, закупки, разработки и внедрения КС, подпадающих под требования надлежащих практик (*GxP*). В принципе, рекомендуется распространить данные процедуры на все подобные системы, имеющиеся в организации.

Следует отметить, что область применения и уровень документации и записей, необходимых для выполнения установленных требований для критических систем, будет зависеть:

- от сложности КС и переменных, влияющих на качество и производительность;
- необходимости обеспечения целостности данных;
- степени риска, сопряженного с работой системы;
- распространения требований надлежащих практик *GxP* на области работы системы.

4.5.4 Документацией, сопровождающей жизненный цикл КС, следует управлять и поддерживать (версии, контрольные следы) в соответствии с общими требованиями к документации и в рамках созданной согласно стандарту качества системы управления документацией. Документация должна быть доступна для предоставления лицам, осуществляющим проверку, по их требованию.

4.5.5 Документация может существовать в различных формах, в том числе на бумажном, электронном или ином носителе.

5 Стадия проекта

5.1 Менеджмент качества

5.1.1 К разработке ПО применимы три основные составляющие обеспечения качества:

- качество, безопасность и эффективность должны быть запроектированы и встроены в ПО;
- качество готового продукта не может быть обеспечено посредством многочисленных испытаний или проверок;
- каждый этап процесса разработки следует контролировать для повышения вероятности соответствия готового ПО всем проектным спецификациям, включая требования к качеству.

5.1.2 Организация должна предпринять все зависящие от нее меры, гарантирующие разработку КС в рамках надлежащей системы менеджмента качества. Поставщик должен быть оценен соответствующим образом.

5.1.3 Пользователи и поставщики должны гарантировать, что ПО и компьютерное оборудование, и системы:

- обладают гарантированным качеством;
- пригодны для предполагаемого использования;
- сопровождаются надлежащей документацией, позволяющей проследить их качество и валидацию.

5.1.4 Существует ряд общепризнанных моделей для процесса разработки ПО, например спиральная модель, каскадная модель (модель "Водопад") и модель жизненного цикла. Каждой из моделей присущи определенные особенности, например: в руководстве по надлежащей практике автоматизированного производства использована *V*-образная модель (см. рисунок 2), однако она не является обязательной для применения[1)].

[1)] В рамках небольших проектов спецификации требований пользователя и функциональные спецификации могут быть объединены. Они будут связаны с квалификацией функционирования.

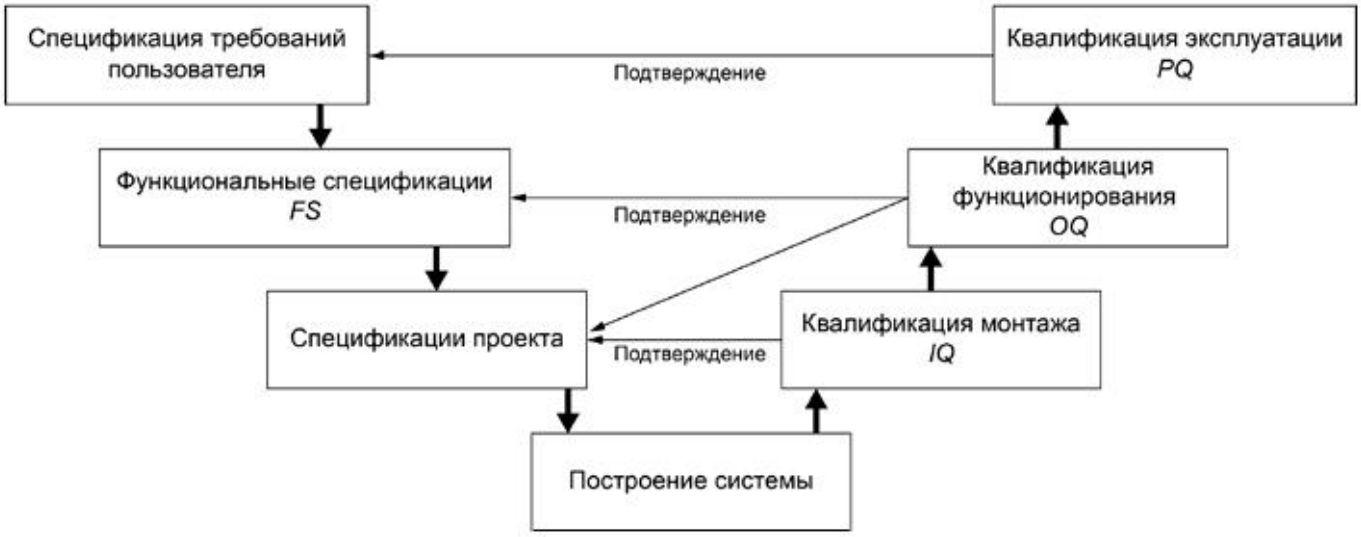

Рисунок 2 - Примерная схема взаимосвязи между ключевыми спецификациями и этапами квалификации в процессе проектирования, построения и тестирования системы [2)]

---

[2] Схема на рисунке 2 приведена лишь в качестве примера. Ожидается, что организация разработает свою модель, учитывающую индивидуальные особенности взаимосвязи между элементами жизненного цикла для данной организации.

На рисунке 2 представлена взаимосвязь между спецификациями требований пользователя и квалификацией эксплуатации *PQ*.

5.1.5 Все процедуры контроля качества и обеспечения качества, документация и записи, относящиеся к разработке и производству программного обеспечения и компьютерного оборудования для компьютерных систем, должны быть в наличии.

5.1.6 Для обеспечения требуемого качества, производительности и надежности КС организация должна гарантировать, что политики управления поставщика, его системы и соответствующие процедуры позволят выполнить эти требования.

5.1.7 Для гарантий качества и надежности КС разработчик ПО должен применять формальный плановый подход, основанный на принципах обеспечения качества при проектировании, разработке, производстве, внедрении и обслуживании, описанных, например, в ГОСТ Р ИСО 9001. Рекомендации по менеджменту качества и элементам системы, включая планы по качеству и управление конфигурацией, приведены в ГОСТ Р ИСО 9004, ГОСТ Р ИСО 10005 и ГОСТ Р ИСО 10007. В [5] приведены конкретные и обязательные требования в отношении планирования. ГОСТ Р ИСО/МЭК 25010 описывает качество ПО и определяет параметры качества для критических приложений. Руководство по надлежащей автоматизированной производственной практике (GAMP) также содержит релевантные для фармацевтической отрасли указания.

В ГОСТ Р ИСО 9001, ИСО/МЭК 25010* и [5][1] представлено несколько положений, критических для обеспечения качества КС:

---

* Вероятно, ошибка оригинала. Следует читать ГОСТ Р ИСО/МЭК 25010. - Примечание изготовителя базы данных.

- КС структурированы исходя из применения системы менеджмента качества к разработке, документирования процессов проектирования, производства и установки продукта;
- соответствие данным стандартам и документу требует наличия в организации формализованных систем для контроля, прослеживаемости и отчетности по продукции и персоналу;
- эти стандарты, а также указанный документ описывают подходы и требования, предъявляемые к производству (изготовлению) ПО согласно модели жизненного цикла, делая упор на важности процедуры контроля за изменениями;
- в стандартах установлена необходимость и важность тестирования ПО, проводимого на нескольких уровнях (фазах):
- тестирование интеграции (интеграционное тестирование);
- тестирование системы;
- приемочное тестирование заказчиком.

---

[1] Руководство GAMP также широко применяется поставщиками и провайдерами, связанными по роду своей деятельности с фармацевтической промышленностью.

5.2 Планирование и управление жизненным циклом

5.2.1 Рекомендации по управлению жизненным циклом КС приведены в ГОСТ Р ИСО/МЭК 12207. Применение принципов, рекомендаций, концепции "жизненного цикла" и надлежащей практики документирования будет способствовать разработке оптимальных систем качества, соблюдению и подтверждению выполнения установленных требований надлежащих практик.

5.3 Спецификации требований пользователя

5.3.1 Спецификации требований пользователя должны описывать необходимые функции КС на основе документально оформленной оценки рисков и влияния с точки зрения соблюдения надлежащих правил. Требования пользователя должны прослеживаться на протяжении всего жизненного цикла КС.

5.3.2 Спецификации должны быть разработаны в соответствии с общими требованиями надлежащих практик к документации, а также:

- каждый документ, содержащий требования, должен быть проверен, утвержден и внесен в реестр документации с уникальной идентификацией;
- устанавливаемые требования к системе не должны противоречить друг другу;
- формулировка каждого требования, в частности необходимого для соответствия надлежащим практикам *GxP*, должна позволять проведение объективной проверки его выполнения с помощью общепринятого метода, например инспекции, анализа или испытания (теста);
- несмотря на независимость спецификаций требований пользователя от поставщика они должны быть согласованы пользователем и поставщиком [2)];

[2)] Данное требование обязательно для КС, изготавливаемых по индивидуальному заказу. Также при приобретении коммерческих настраиваемых и конфигурируемых систем будущие пользователи, интеграторы и поставщики должны обсудить и рассмотреть разработанные требования пользователя и степень их удовлетворения предполагаемым программным обеспечением. Необходимо определить "степень удовлетворения" и контролировать ее соблюдение при проведении необходимых работ по конфигурации, модификации, кодировании и тестировании, валидации.

- обязательные регуляторные требования и опциональные параметры должны быть четко разделены;
- в спецификации требований пользователя должны быть указаны функциональные и нефункциональные требования к системе: функциональность, эффективность, возможность обслуживания, удобство эксплуатации и т.п.; формулировка каждого требования должна позволять проведение объективной проверки его выполнения.

5.3.3 Спецификации должны быть разработаны в первую очередь на ПО. Также должны быть установлены требования к компьютерному оборудованию и другие требования (например, по наличию письменных процедур).

5.3.4 Функционал спецификаций требований пользователя и функциональных спецификаций должен гарантировать выполнение соответствующих требований надлежащих практик *GxP*, а также содержать информацию о наличии критических интерфейсов между системой и ручными операциями.

5.3.5 Спецификации составляют основу для оценки рисков системы в отношении соблюдения надлежащих практик *GxP*, а также других рисков, например, безопасности. Анализ рисков может быть основан на функциональной спецификации, связанной со спецификациями требований пользователей (например, в случае КС, изготовленных по индивидуальному заказу). Оценка рисков, а также ее результаты, включая критерии ранжирования рисков на критические или некритические, должны быть задокументированы. Источники любых рисков, связанных с соблюдением надлежащих практик *GxP*, должны быть определены.

5.3.6 Спецификации требований пользователя или ссылка на них могут быть включены в документ, описывающий КС (см. 4.5.1), вместе с результатами оценки рисков на стадии разработки спецификации.

5.3.7 При выборе коммерческого обеспечения или компонента спецификации требований пользователя могут быть разработаны на основе спецификации поставщика.

5.3.8 Все КС следует подвергать документированной перспективной валидации или квалификации (см. 5.6.7 для определения подходов к валидации различных типов КС), при необходимости, повторной валидации или квалификации. Спецификации требований пользователя и документ, содержащий описание системы, должны актуализироваться как подтверждение нового этапа валидационного жизненного цикла.

5.4 Функциональная спецификация FS

5.4.1 Функциональная спецификация разрабатывается поставщиком КС на основании спецификации требований пользователя - в случае индивидуально разрабатываемого ПО или определяется для выбора и приобретения серийного программного продукта. Функциональная спецификация должна описывать систему, отвечающую спецификации требований пользователя, то есть потребностям организации.

5.4.2 Данная спецификация должна содержать точное и детализированное описание всех необходимых требований к компьютерной системе и интерфейсам, то есть описание функций, работы системы и, где применимо, ограничения проекта и характеристики.

5.4.3 Для определенных типов и уровней системы могут быть разработаны комбинированные спецификации, включающие требования пользователя и функциональные требования (см. 5.6.7 для определения подходов к валидации различных типов КС).

5.4.4 Организация должна иметь в наличии документацию, описывающую компьютерную систему с приложением, если возможно, диаграмм потока или блоков, показывающих раскладку оборудования, сети и взаимодействия. Эти схемы должны быть совместимыми с функциональной спецификацией и прослеживаемыми до спецификации требований пользователя. Данная документация является частью описания КС (см. 4.5.1).

5.5 Тестирование

5.5.1 Обеспечение надежности ПО достигается выполнением планов качества и тестированием[1)] в процессе разработки. В процессе разработки проводят тестирование компонентов и интеграции в соответствии с принципами, изложенными в ГОСТ Р ИСО 12207*, [5] и [6][2)].

---

1) Тестирование представляет собой верификацию компонента ПО. Верификация в контексте жизненного цикла представляет собой совокупность действий по сравнению полученного результата жизненного цикла с требуемыми характеристиками для этого результата.

2) См. также соответствующие разделы руководства GAMP.

* Вероятно, ошибка оригинала. Следует читать: ГОСТ Р ИСО/МЭК 12207. - Примечание изготовителя базы данных.

5.5.2 Тестирование, так же как и разработку ПО и компьютерного оборудования системы, следует проводить в условиях системы менеджмента качества, задокументированным образом и формально согласованным всеми сторонами. При определении мест проведения тестирования и ответственности сторон рекомендуется использовать соответствующие рекомендации руководства GAMP.

5.5.3 Тестирование интеграции является одним из важнейших этапов разработки ПО, проводимое на протяжении интеграции компонентов КС и до полной интеграции всей системы. По мере создания элементов программы, предпочтительно до сдачи блока (модуля) программы на формальное тестирование, рекомендуется проводить систематические проверки исходного кода программы, включая оценку критических алгоритмов и стандартных элементов.

5.5.4 Результаты функционального тестирования могут подтвердить надежность простых КС, таких как программно-логические контроллеры и системы, основывающиеся на базовых алгоритмах и наборах логических блоков. Для критически важных и (или) более сложных систем верификационное тестирование, выполняемое в ходе квалификации монтажа, функционирования и эксплуатации, не обеспечивает требуемой степени уверенности в надежности выполнения системой предназначенной функции, так как не обеспечивает полную оценку скрытых функций и программного кода.

5.5.5 Для подтверждения надлежащей установки (инсталлирования) системы, ее функционирования и производительности следует использовать документально оформленные сценарии[3] (спецификации процедуры тестирования). Данные сценарии должны быть соотнесены со спецификациями требований пользователя и функциональными спецификациями системы, в частности, должны быть рассмотрены пределы параметров системы (процесса), границы данных и обработка ошибок[4]. При применении автоматизированных средств тестирования и тестовых сред должна быть проведена и задокументирована оценка их пригодности для тестирования проверяемой системы.

---

[3] В Правилах надлежащей производственной практики используется термин "схемы тестирования".

[4] В соответствии с собственным планом качества проекта для подтверждения работы системы в соответствии с функциональными спецификациями разработчик/провайдер разрабатывает проекты сценариев тестирования. Сценарий должен обеспечивать проведение стрессового тестирования структурной целостности, критических алгоритмов и "предельных значений" интегрированного ПО. Обеспечение взаимосвязи сценариев тестирования со спецификациями требований потребителя является ответственностью организации, работающей в условиях надлежащих практик *GxP*.

5.5.6 Для любого технологического оборудования и процессов, связанных или контролируемых посредством компьютерных систем, потребуются дополнительные режимы испытаний при квалификации монтажа, квалификации функционирования и квалификации эксплуатации. Допускается объединение этапов тестирования и областей тестирования для однородной группы оборудования и процессов; данный подход должен быть указан в плане или протоколе тестирования.

5.5.7 Организация должна продемонстрировать доказательства формализованной приемки системы после ее тестирования и контролируемого переноса в функционирующее операционное окружение.

5.6 Валидация

5.6.1 Валидацию проводят для получения объективных и документальных свидетельств о том, что компьютерная система и КС будут постоянно функционировать как установлено в спецификациях, внедрены и провалидированы.

Организация должна быть способна предоставить свидетельства того, что используемые КС демонстрируют рабочие диапазоны, сложность, функциональность, управляемость и валидированный статус.

5.6.2 Для целей валидации КС организация должна иметь систему, обеспечивающую проведение формальной оценки и ведение отчетности о качестве и производительности КС на всех этапах ее жизненного цикла: разработки, внедрения, квалификации, приемки, функционирования, модификации, повторной квалификации, обслуживания и демонтажа.

Валидационная документация и отчеты должны охватывать соответствующие стадии жизненного цикла КС. Производитель должен обосновать свои стандарты, протоколы, критерии приемлемости, процедуры и записи на основе оценки рисков.

Валидационная документация должна включать записи контроля изменений (если применимо) и отчеты о любых отклонениях, выявленных в ходе процесса валидации.

Валидационную документацию можно вести в электронном или бумажном виде. Связанные валидационные досье для компонентов сложной КС должны быть снабжены четкими перекрестными ссылками для целей аудита.

5.6.3 В перечне (реестре) КС (см. также 4.1.3), эксплуатируемых организацией, должно быть указание валидационного статуса; подробное описание объема (степени) валидационных работ приведено в сводной документально оформленной программе валидации[1)]. Описание объема валидации должно включать критерии соответствия надлежащим практикам *GxP* с указанием критичности рангов рисков для качества продукта/процесса и целостности данных (в случае сбоя системы или ее выхода из строя).

[1)] Объем (степень) валидационных работ может быть указан в отдельных валидационных планах. Может быть использована иерархия связанных валидационных планов, описанная в рекомендациях по планированию валидации руководства GAMP.

5.6.4 Подтверждение соответствия требованиям надлежащих практик *GxP* критично для различных операций и работ, при которых используют КС: ввод данных (захват и целостность), запись данных в файл, обработка данных, работа с информационными сетями, управление процессом и его мониторинг, электронные записи, архивирование, восстановление данных, печать, доступ, управление изменениями, контрольные следы и решения, связанные с любой автоматизированной деятельностью, выполняемой в условиях надлежащих практик к *GxP*. Например, создание и представление регистрационных досье и других документов в регуляторный орган, исследования и разработка лекарственных средств, клинические исследования, материально-техническое снабжение, отпуск в производство (взвешивание), производство, упаковка, испытания, контроль качества, обеспечение качества, управление запасами, хранение и поставки лекарственных средств, обучение, поверка и калибровка (и проверка работоспособности), техническое обслуживание, контракты (технические соглашения) и связанные с этими работами записи и отчеты (данный перечень не является исчерпывающим).

5.6.5 Определение рисков КС для качества представляет собой одну из наиболее важных предварительных работ при разработке основного валидационного плана КС. Анализ рисков систем и его результаты, одновременно с обоснованием системы ранжирования рисков на критичные и некритичные, должны быть оформлены документально. Кроме того, должны быть четко определены потенциальные риски для соответствия требованиям надлежащих практик *GxP*. Критические системы (и функции внутри систем), обладающие наибольшим потенциалом причинения вреда в случае их сбоя или выхода из строя, относят к приоритетным.

5.6.6 Политика в области валидации или основной валидационный план организации должен содержать описание используемых организацией подходов к валидации и управлению КС. Основной валидационный план должен включать (или содержать ссылки на другие документы, отдельные валидационные планы, письменные процедуры):

- перечень КС, подлежащих валидации;
- краткое описание подходов к валидации для различных типов КС и проводимых валидационных работ;
- описание протоколов (планов) и соответствующих процедур тестирования для всех валидационных работ, относящихся к компьютерным системам;
- требования к валидационным отчетам, документирующим валидационные работы и полученные результаты;
- указание ответственного персонала и степень их ответственности в рамках программы валидации.

5.6.7 В соответствии с руководством GAMP выделяют пять типов ПО и соответствующие подходы к их валидации (см. таблицу 1).

Таблица 1 - Типы программного обеспечения и подходы к валидации

Категория	Тип программного обеспечения	Валидационный подход
1	Операционная система	Регистрация информации о версии (включая сервисные дополнения). Тестирование будет осуществлено опосредованно, путем функционального тестирования приложения
2	Встроенное ПО	Для неконфигурируемого встроенного ПО - регистрация информации о версии. Проверка работоспособности (калибровка) оборудования по мере необходимости. Подтверждение надлежащего функционирования в соответствии с требованиями пользователя
		Для конфигурируемого встроенного ПО - регистрация информации о версии и конфигурации. Проверка работоспособности (калибровка) оборудования, по мере необходимости, и подтверждение надлежащего функционирования в соответствии с требованиями пользователя
		Встроенное ПО, разработанное по индивидуальному заказу, относится к категории 5
3	Стандартный пакет ПО	Регистрация версии (и конфигурации операционного окружения) и подтверждение надлежащего функционирования в соответствии с требованиями пользователя. Для критически важных и комплексных приложений следует оценить необходимость аудита поставщика

4	Конфигурируемый пакет ПО	Регистрация версии и конфигурации и подтверждение надлежащего функционирования в соответствии с требованиями пользователя. В большинстве случаев следует проводить аудит поставщика для критически важных и комплексных приложений
		ПО, разработанное по индивидуальному заказу, относится к категории 5
5	ПО, разработанное по индивидуальному заказу	Аудит поставщика и валидация всей системы

Приведенная в таблице 1 классификация может быть неприменима к сложным интегрированным КС, в которых одновременно можно выделить различные типы программ. Для определения подходов к валидации любой критической системы следует применять комплексный подход, основанный на оценке всех рисков при использовании данного приложения. Для каждого компонента КС оценка рисков помогает определить подходы по обеспечению качества, работы по квалификации и меры по снижению рисков. Информация об анализе рисков, подходах к выявлению рисков несоответствия надлежащих практик *GxP* и критериях оценки пригодности для использования системы должна быть доступна для предоставления лицам, осуществляющим проверку, по их требованию.

5.6.8 Валидационная документация и записи также должны включать следующие данные о контроле системы, мониторингу и техническому обслуживанию:

- оценка результатов испытаний на соответствие спецификаций требований пользователя (этап верификации и текущий мониторинг);
- записи об обучении операторов (вводный инструктаж и периодическое обучение);
- процедура текущего мониторинга (данная процедура будет связывать систему отчетов об ошибках и систему отчетов об отклонениях с процедурой управления изменениями);
- поддержание руководств пользователя и стандартных операционных процедур (СОП) для всех систем в актуальном состоянии.

5.6.9 Операционные системы и встроенное ПО квалифицируют в зависимости от предполагаемого использования [принимая во внимание версию, устойчивую версию (релиз) или релевантные параметры] в рамках квалификации эксплуатации *PQ*/валидации процесса.

5.6.10 Если данные переводят в другой формат или систему данных, валидация должна включать проверку неизменности значения и смысла данных в процессе их миграции.

5.6.11 Помимо приемочных испытаний (квалификация функционирования) в соответствии с функциональной спецификацией, которые могут включать в себя заводские приемочные испытания [процессно-аналитическая технология, Process Analytical Technology (PAT)], проводимые, например, на стороне поставщика, организация несет ответственность за квалификацию эксплуатации системы. В данном контексте приемо-сдаточные испытания [приемочные испытания на площадке, Site Acceptance Test, (SAT)], проводимые организацией при квалификации эксплуатации системы в ее операционном окружении, должны быть осуществлены в соответствии со спецификацией требований пользователя, в которую будут включены протоколы и критерии приемлемости производительности и качества как контролирующей системы, так и контролируемого (имеющего отношение к фармации) процесса. В последнем случае должны быть приведены перекрестные ссылки на любую релевантную валидационную документацию.

5.6.12 Организация должна обеспечить доступность документированных валидационных данных, которые должны быть доступны для предоставления лицам, осуществляющим проверку, по их требованию.

Ретроспективная валидация

5.6.13 Ретроспективная валидация не является эквивалентом перспективной валидации и не применима для вновь устанавливаемых КС. Однако в некоторых случаях организации необходимо продолжать эксплуатацию системы, не подвергавшейся перспективной валидации при установке. Для использования такой системы в условиях надлежащих практик *GxP* организация должна разработать описание и оформить документально проверку/тестирование системы на соответствие спецификации требований потребителей и других спецификаций с использованием предшествующих данных (журналов регистрации ошибок, внесенных изменений, руководств пользователя и процедур), а также анализ критичности и рисков системы, оценку поставщика.

5.6.14 Стабильная и надежная работа большинства ранее установленных невалидированных систем не является основанием для отказа от проведения их валидации[1)]. Проведение ретроспективной валидации допустимо для ранее установленных систем (до внедрения правил надлежащих практик *GxP* в организации) или при переводе системы в категорию *GxP* КС.

---

1) Учитывая, что в надлежащих практиках *GxP* требования о валидации КС существует уже достаточно давно, регуляторные органы могут рассматривать отсутствие данных о проведении перспективной валидации нарушением установленных требований. Часто ранее установленные системы не отвечают приведенным в надлежащих практиках требованиям, и организации вынуждены их заменять или модифицировать.

5.6.15 Указанные выше принципы валидации компьютерных систем должны быть учтены при проведении ретроспективной валидации. Документация по разработке, а также записи, пригодные для проведения валидации ранее установленных систем, могут быть недоступны ввиду длительности их использования и уникальных характеристик, поэтому подход к установлению и документированию надежности системы и гарантий ее качества, основанный на концепции "встроенного качества" на этапе разработки ПО, будет отличаться для новых современных и ранее установленных систем.

5.6.16 При проведении ретроспективности валидации КС применяются общие принципы ретроспективной валидации, основанной на формализованной оценке данных предшествующих периодов об использовании системы, технического обслуживания, отчетов об ошибках и записей системы управления изменениями, а также оценке рисков системы и ее функций. Оценку проводят с использованием документально оформленных спецификациях требований пользователя[2]. В том случае, если предшествующие данные не охватывают текущий диапазон параметров функционирования или при существенных изменениях работы системы, ретроспективные данные не могут быть использованы для валидации текущей версии системы.

---

[2] Для ретроспективной разработки спецификаций требований пользователя, в большом количестве случаев, использовались отчеты об опыте работы с системой, подкрепленные дополнительным тестированием.

5.6.17 Проведение валидации в рамках текущей оценки (верификации) ранее установленных систем должно повлечь за собой применение к ней требований процедур, документации, записей в отношении современных КС, в том числе управление изменениями, контрольные следы (при необходимости), безопасность данных и системы, дополнительная разработка и модификация ПО в условиях системы менеджмента качества, поддержание целостности данных, требования к резервному копированию системы, обучение операторов (пользователей) и постоянная текущая оценка функционирования системы.

5.6.18 Отсутствие адекватных свидетельств проведения ретроспективной квалификации или валидации должно служить основанием для приостановления, прекращения использования или отключения любой ранее установленной(ых) системы (систем).

6 Стадия эксплуатации

6.1 Данные

6.1.1 КС, осуществляющие электронный обмен данных с другими системами, должны включать соответствующие встроенные средства контроля правильного и безопасного ввода и обработки данных с целью минимизации рисков.

6.1.2 Организация должна вести записи проверок того, что интерфейс(ы) данных/управления/мониторинга между системой и оборудованием обеспечивает(ют) корректный ввод и вывод.

6.1.3 При ведении системы документации в электронном виде и использовании электронных подписей рекомендуется вести реестр авторизованных пользователей, кодов идентификации, области авторизованных действий (степени доступа).

6.1.4 Используемые системы электронной обработки данных должны обеспечивать следующие меры по защите данных:

- доступ только для авторизованного персонала;
- использование паролей;
- создание резервных копий;
- независимая проверка критических данных;
- безопасное хранение данных в течение требуемого промежутка времени.

Также применяемые в организации системы электронных записей должны быть провалидированы. В таких системах, если возможно, должны быть предусмотрены системы контрольных следов.

6.1.5 При выборе организацией ведения документации в электронной форме следует определить все применимые в данном случае регуляторные требования, степень юридической значимости электронных записей и эквивалентности своим бумажным аналогам. Отдельные разделы надлежащих практик *GxP* могут содержать особые регуляторные требования, например для тех случаев, когда электронные записи и подписи использованы в качестве источника первичных исходных данных, записей и/или свидетельств.

Организация должна пояснить и обосновать применение используемых информационных технологий и методов контроля.

Подходящая форма электронной подписи[1)] или аутентификации/идентификации[2)] должны применять в следующих случаях:

- к компьютеризированной *GxP*-системе допускается доступ извне;
- система генерирует регуляторные *GxP*-записи в электронном виде;
- ключевые решения и действия могут быть реализованы при помощи электронного интерфейса.

---

1) Электронная подпись должна быть уникальной для пользователя, но не обязательно быть уникальной для системы. Кроме того, выпуск единой электронной подписи для целого ряда систем также может представляться более удобным. Организация должна пояснить и обосновать эти принятые решения, их логику, а также методы контроля.

2) Организация должна обосновать выбор методов, обеспечивающих соблюдение требований надлежащих практик *GxP*.

6.1.6 В некоторых системах (так называемых "гибридных") может быть использована комбинация ручного управления и автоматизированных функций, а также широкий набор средств для обработки *GxP*-данных, а также записей и информации. В подобных случаях при совместном использовании записей на бумажном носителе (в т.ч. распечаток КС) и электронных файлов для полноценного ведения журнала контрольных следов могут потребоваться документированные процедуры контроля с записанными ссылками и подписями.

6.1.7 К ключевым аспектам инфраструктуры, системы и конкретных приложений, которые необходимо контролировать, относятся:

- авторизованный доступ пользователя к конкретному приложению;
- уникальная комбинация идентификатора пользователя и пароля, запрашиваемая КС и связанная с авторизованной учетной записью пользователя для применения в конкретном приложении;
- разрешенный функционал для конкретного пользователя;
- определенный часовой пояс и стандарт даты, связанный с относительной ссылкой транзакций (сложные системы могут находиться более чем в одном часовом поясе);
- контрольные следы;
- прочие физические и логические способы контроля инфраструктуры информационной безопасности.

6.1.8 При использовании "открытых" КС (т.е. систем с возможностью доступа извне, иногда такие системы называют "открытыми") должны быть соблюдены следующие требования.

В "открытой" системе имеется механизм, обеспечивающий доступ извне и соответствующий ввод данных только для авторизованных клиентов, при этом данные поступают в корректном формате, например в виде зашифрованной почты с цифровой подписью, или как пакет данных. Также в системе встроена функция карантина полученных извне данных в случае несоблюдения условия безопасности. Порядок управления информационной безопасностью должен включать карантин подобных данных, уведомление об их поступлении, а также принятие в их отношении окончательного решения.

Система обеспечивает регистрацию и прослеживание всех внешних входов в нее. Каждый элемент этапа обработки должен включать в себя механизмы входа в элемент системы и мониторинга. Для надлежащим образом защищенных систем, а также для доступа в режиме "только чтение" может использоваться менее сложный метод прослеживания.

Система обладает возможностями хранения копий данных и их повторной пересылки с одной стадии на другую в случае их "потери" или повреждения на последних этапах обработки.

6.1.9 Для компьютеризированных *GxP*-систем, которые генерируют регуляторные записи в электронном виде, позволяют осуществлять доступ извне или принимать ключевые решения и предпринимать действия посредством электронных интерфейсов, требуются дополнительные схемы безопасности и способы контроля. Данные требования предопределены в основном международными инициативами в сфере электронной торговли. Тем не менее когда компании связывают подобные открытые системы (с возможностью доступа извне) со своими *GxP*-системами, информация о безопасности, способах контроля и валидации должна быть задокументирована и доступна при инспектировании.

6.2 Контроль правильности ввода данных

6.2.1 Для критических данных, например технологических записей, данных лабораторных испытаний, а также записей, переносимых с бумажных носителей, в том числе вводимых вручную, необходимо предусмотреть дополнительный контроль точности ввода данных.

Этот контроль может осуществляться вторым оператором или с помощью валидированных электронных средств. Второе авторизованное лицо с идентифицированным именем входа (логином) и идентификатором, а также с зарегистрированной датой и временем может проверить введенные данные при помощи клавиатуры. Для автоматизированных систем, включающих в себя непосредственный захват данных и связанных с другими базами данных и интеллектуальной периферией, вторая проверка может являться частью валидированной функции системы (например, при выдаче материала в производство). Для обеспечения подобной проверки можно использовать особый доступ, функции управления системой и/или специализированные устройства, например идентификационные штрих-коды, а также включение и использование контрольных следов для регистрации всевозможных изменений, которые потенциально могут повлиять на данные.

6.2.2 Критичность и потенциальные последствия ошибочного или неправильного ввода данных в систему должны быть охвачены системой управления рисками.

6.3 Хранение данных

6.3.1 Данные должны быть защищены от повреждений как физическими, так и электронными мерами. Сохраненные данные должны проверять на доступность, читаемость и точность. Доступ к данным должен быть обеспечен на протяжении всего периода их хранения.

6.3.2 Следует выполнять регулярное резервное копирование всех необходимых данных.

Организация должна разработать и применять валидированные процедуры резервного копирования, регламентирующие в том числе системы хранения и носители информации. Частота резервного копирования зависит от функций компьютерной системы и оценки рисков потери данных. С целью гарантирования доступности сохраненных данных должны быть созданы резервные копии данных, необходимых для восстановления всей *GxP* документации (в том числе записи контрольных следов).

Сохранность и точность резервных копий, а также возможность восстановления данных должны быть проверены в процессе валидации и периодически контролироваться.

6.3.3 Организация должна иметь письменные процедуры восстановления КС после сбоя. Для обеспечения извлечения и поддержания *GxP*-информации данные процедуры должны включать в себя требования, предъявляемые к документации и записям. К процедурам резервного копирования и восстановления системы после сбоя предъявляются следующие основные требования:

- процедуры должны обеспечивать плановое резервное копирование данных в безопасные места хранения, надлежащим образом отделенные от основного места хранения, при этом частота копирования должна быть основана на анализе рисков для *GxP*-данных;
- процедура резервного копирования, а также системы хранения и носители должны обеспечивать целостность данных. Должен существовать журнал учета данных, подвергнутых резервному копированию, с указанием используемых для хранения носителей. Используемые носители должны быть задокументированы, а их надежность обоснована;
- все *GxP*-данные, в том числе журналы контрольных следов, следует подвергать резервному копированию;
- процедуры резервного копирования и восстановления должны подвергать регулярному тестированию согласно письменной процедуре, содержащей план тестирования;
- должны вести журнал учета тестирования процедуры резервного копирования, включающий дату тестирования и его результаты, а также записи устранения любых ошибок.

6.4 Распечатки

6.4.1 Необходимо иметь возможность получения четких печатных копий данных, хранящихся в электронном виде.

Для записей, сопровождающих разрешение на выпуск серии, должна быть предусмотрена возможность получения распечаток, фиксирующих наличие или отсутствие изменений данных с момента их первоначального ввода.

6.5 Контрольные следы (autotrail)

6.5.1 На основе оценки рисков необходимо уделить внимание встраиванию в систему возможности создания записей всех существенных изменений и удалений, связанных с областью действия надлежащих правил (система, создающая контрольные следы). Причины таких связанных с надлежащими правилами изменений или удалений данных должны быть оформлены документально. Контрольные следы должны быть доступными, иметь возможность их преобразования в понятную для пользователей форму и регулярно проверяться.

6.5.2 В случае необходимости контрольные следы целостности данных могут включать в себя, помимо прочего, такие функции, как создание, ссылки, встроенные комментарии, удаления, модификации/коррективы, полномочия пользователей, время и дату. Все связанные компоненты должны быть неизменяемо связаны в рамках контролируемых контрольных следов системы безопасности ИТ-системы. Все исходные записи данных и коды, а также любые последующие изменения, дополнения, удаления или модификации должны быть тщательно и в полном объеме сохранены в доступных контрольных следах. Источники и содержание транзакций, фиксируемых в контрольных следах, должны основываться на утвержденных процедурах организации по управлению информационной безопасностью данных для конкретного компьютеризированного приложения и полномочий пользователя. Рекомендуется использование системного контекстуального маркирования транзакций в электронных контрольных следах, так как они могут содержать автоматизированные функциональные обратные контрольные связи с параметрами валидации безопасности.

Рекомендации по разработке, внедрению и контролю системами контрольных следов приведены в ГОСТ Р ИСО/МЭК 27002.

6.5.3 Записи, относящиеся к событиям, фиксируемым в контрольных следах, должны документировать, желательно, автоматически, посредством функции операционной системы, системы управления базой данных, системой управления документацией и с помощью прочих основных приложений. При необходимости должны быть доступны записи контрольного журнала в удобочитаемой форме.

6.6 Управление изменениями и конфигурацией

6.6.1 Любые изменения в КС, включая конфигурацию системы, должны проводить только контролируемым способом в соответствии с установленной процедурой. Процедура управления изменениями в КС должна быть интегрирована в общеорганизационную процедуру управления изменениями организации.

На раннем этапе проектирования может быть достаточно ведения записей, содержащих актуальную информацию о проекте, без необходимости подтверждения изменений, однако после начала разработки спецификаций и утверждения основных характеристик внесение изменений проводят в соответствии с действующей процедурой управления изменениями, предусматривающей четкое и контролируемое внесение изменений и их документирование и определяющей ответственность лиц, участвующих в управлении изменениями.

Процедура управления изменениями КС должна содержать требования в отношении:

- подробных записей, касающихся предлагаемого изменения(ий), с обоснованием;
- статуса системы и влияния на контроль до внедрения изменения(ий);
- порядка согласования и утверждения изменений (см. 6.6.7);
- записей, касающихся согласования изменений и принятых решений (одобрено или отклонено);
- порядка указания статуса "изменено" в документации;
- подхода(ов) и метода(ов) оценки полного влияния изменения(ий), включая регрессионный анализ и регрессионное тестирование, при необходимости стандарты института инженеров электрики и электроники (Institute of Electrical and Electronics Engineers, IEEE);
- взаимодействия процедуры внесения изменений с системой управления конфигурацией.

6.6.2 Управление изменениями следует осуществлять на всех этапах жизненного цикла КС, то есть от стадий проекта и разработки до эксплуатации, технического обслуживания, модификаций и изъятия из обращения. Соответствующие указания должны быть приведены в валидационных планах. Записи об изменениях следует хранить вместе с другими документами о КС.

6.6.3 Процедура управления изменениями КС должна учитывать соответствующие процедуры и записи поставщиков, интеграторов и других сторон, участвующих в поддержке конкретной системы и приложений. В крупных организациях со сложной внутренней структурой допускается использование децентрализованных валидированных процедур управления изменениями в КС.

6.6.4 Процедура должна учитывать любые изменения, происходящие вследствие усовершенствования системы, т.е. изменений, внесенных в спецификации требований пользователя и не идентифицированных в начале проекта. Также изменение может быть результатом корректирующих действий или исправления ошибки, отклонения или проблемы, выявленной в ходе использования системы. Процедура должна описывать порядок и документальные требования для внесения экстренных изменений (хотфиксов, текущих исправлений). Каждая ошибка и утвержденные действия должны быть подробно задокументированы. Данные записи могут существовать как на бумаге, так и в электронном виде.

6.6.5 Следует определить, что изменение в КС и ее описание могут потребоваться:

- после отчета об отклонении;
- отчета об ошибке;
- запроса на улучшение компьютерной системы;
- обновления аппаратного или программного обеспечения.

6.6.6 Процедуры систем качества должны обеспечивать подробную документацию изменений и фиксацию завершения работ по их внесению. Процедура управления изменениями должна быть тесно связана с системой управления отклонениями и ошибками[1)].

[1)] Приложения руководства GAMP по аспектам эксплуатации КС содержат рекомендации по данным вопросам.

6.6.7 Поставщик ПО должен иметь собственную систему управления изменениями, при этом должны существовать четкие и согласованные процедуры, описывающие взаимодействие между системами управления изменениями поставщиков и пользователей. Согласованные изменения вносят контролируемым способом в соответствии с действующей документацией системы качества, требованиями процедур и ведением записей.

6.6.8 Изменения в валидированную КС не должны вносить без рецензирования и утверждения со стороны всех заинтересованных сторон, ответственных за выполнение текущих требований пользователя, например владельца системы и представителя отдела обеспечения качества. Для проверки приемлемости элемента ПО, разработанного в ответ на запрос о внесении изменения, должны использовать сценарии тестирования (конкретного типа и объема), определенные планом проекта внесения изменений. Перед выпуском новой версии ПО может потребоваться тестирование интеграции. При этом в особых случаях возможны рассмотрение предлагаемых изменений в качестве инфраструктурных и определение круга заинтересованных сторон.

6.6.9 Общие функции информационно-технологической инфраструктуры могут потребовать централизованного контроля со стороны подразделения по ИТ-системам и управлению информационной безопасностью. Основные функции, ответственность и процедуры должны быть задокументированы в соответствующих соглашениях об уровне услуг (внутренних или внешних) или аналогичных документах.

6.7 Периодическая оценка

6.7.1 Относительно КС следует проводить периодическую оценку для подтверждения их валидированного состояния и соответствия требованиям надлежащих правил. Такие оценки должны включать, в случае необходимости, оценку текущего диапазона функциональных возможностей, записей отклонений, сбоев, проблем, истории обновлений, отчеты об эксплуатации, надежности, защищенности и о валидационном статусе.

6.8 Защита

6.8.1 Защита КС и данных является критичной, надлежащие процедуры и записи должны основываться на ИТ-политике пользователя и соответствовать установленным регуляторным требованиям. Управление доступа к системам включают в обязанности "владельца системы", при этом для критических КС контроль должен быть реализован при помощи системы управления информационной безопасностью.

Должна быть установлена четкая ответственность за управление безопасностью системы, пригодная как для малых, так и для сложных систем, в том числе:

- за реализацию стратегии безопасности и делегирование полномочий;
- управление и присвоение полномочий в системе;
- установление уровней доступа пользователей;
- управление уровнями доступа к инфраструктуре (фаерволл, резервное копирование, перезапуск серверов, системы и т.п.).

6.8.2 Для обеспечения доступа к КС только лицами, имеющими на это право, необходимо использовать физические и (или) логические элементы контроля. Соответствующие способы предотвращения несанкционированного доступа к системе могут включать в себя использование ключей, карточек доступа, персональных кодов с паролями, биометрических данных, ограничения доступа к компьютерному оборудованию и зонам хранения данных.

Степень защиты зависит от критичности КС.

6.8.3 Создание, изменение и аннулирование прав доступа должно быть зарегистрировано.

Следует разработать систему управления данными и документами для идентификации операторов, осуществляющих вход, а также для регистрации изменения, подтверждения или удаления данных, включая дату и время.

Имеющиеся в организации процедуры и записи должны удовлетворять следующим требованиям:

- права доступа (как физического, так и логического) для всех операторов четко определены и контролируются;
- основные правила по защите КС, данных, личных паролей или карт доступа оформлены документально и соответствуют требованиям надлежащих практик *GxP*;
- на соответствующих организационных уровнях установлены надлежащие полномочия и ответственность;
- письменно установлен порядок периодической проверки кодов идентификации и паролей, их пересмотра и аннулирования, в том числе после установленного количества неудачных попыток входа в систему;

- определена процедура управления потерянными данными для электронного аннулирования потерянных, украденных или потенциально скомпрометированных паролей, а также принудительной периодической смену* паролей. Конкретная частота смены паролей должна быть обоснована в рамках системы управления информационной безопасностью;

_____

* Текст документа соответствует оригиналу. - Примечание изготовителя базы данных.

- процедуры обеспечивают выявление запрещенных паролей;

- ведется журнал попыток взлома парольной защиты, в отношении данных попыток предусмотрено проведение расследования и принятие необходимых мер;

- приняты меры по обеспечению валидированного восстановления исходной информации и данных после резервного копирования, перезаписи со сменой носителя, транскрипции, архивирования или сбоя в системе;

- создан реестр оборудования, не имеющего необходимых возможностей для логической защиты (паролей), например отдельных КС, интерфейсов между оборудованием и оператором, и инструментов, и предусмотрены другие процедуры защиты.

6.8.4 Для обеспечения в экстренных случаях доступа регуляторных органов к зашифрованным данным организации должны быть созданы готовые ключи для расшифровки, либо процесс расшифровки должен быть проведен под надзором проверяющего лица.

6.8.5 Должна быть обеспечена также физическая безопасность системы для того, чтобы минимизировать возможность несанкционированного доступа, а также намеренного или случайного повреждения персоналом либо потери данных.

6.9 Управление инцидентами

6.9.1 Все инциденты (непредвиденные случаи), включая системные сбои и ошибки данных, должны быть записаны и оценены. Необходимо установить основную причину критических сбоев и использовать эту информацию в качестве основы корректирующих и предупреждающих действий.

6.9.2 Валидированные и защищенные электронные системы обработки данных могут быть использованы для целей регистрации в реестре того, что серия продукции соответствует требуемым стандартам.

6.10 Электронная подпись

6.10.1 Электронные записи могут быть подписаны в электронном виде. Электронные подписи должны:

а) в рамках организации иметь такое же значение, как рукописные подписи;

б) быть неразрывно связанными с соответствующими записями;

в) включать время и дату, когда они были поставлены.

6.10.2 При использования электронных подписей в условиях надлежащих практик *GxP* необходимо обеспечить следующее:

- наличие документированных свидетельств соответствия всех аспектов инфраструктуры, системы и конкретных приложений установленным требованиям;
- принятие адекватных мер по защите ключа к цифровой подписи в тех случаях, когда оценка рисков выявила необходимость использования цифровой подписи (например, при участии в выпуске в обращение третьей стороны или сборе и передаче первичных клинических данных в условиях надлежащей клинической практики). Необходимый уровень защиты будет зависеть от критичности транзакции и рисков при неавторизованном использовании ключа. Если при оценке рисков была выявлена потребность в высоком уровне защиты может потребоваться использование инфраструктуры открытых ключей;
- ведение реестра авторизованных лиц;
- наличие процедур, обеспечивающих информирование лиц, авторизованных для использования электронных подписей, об ответственности за действия, совершенные с использованием их электронных подписей;
- наличие у персонала, отвечающего за администрирование системы, необходимых допусков по безопасности, а также подтверждение соответствующего обучения, надлежащих знаний и навыков;
- наличие процедур записи напечатанного имени или "проверки подлинности" подписывающего лица, даты и времени подписания документа, а также значения, связанного с подписью;
- наличие процедур, направленных на предупреждение неавторизованного использования электронной подписи или скомпрометированных комбинаций идентификатора и пароля.

6.10.3 При использовании электронных записей для архивирования *GxP*-данных необходимо обеспечить следующее:

- наличие документированных свидетельств соответствия;
- наличие процедур архивирования и соответствующих записей;
- наличие процедур, обеспечивающих правильность, надежность и стабильность электронной системы записей в соответствии с результатами валидационного испытания (см. 6.7);
- использование способов контроля и мер (установленных соответствующими процедурами) для идентификации, изоляции и сообщения о некорректных или поврежденных записях;
- наличие процедур, позволяющих получать доступ к записям на протяжении всего периода хранения;
- возможность создания точных и полных копий записей как в электронной, так и удобочитаемой для человека форме;
- доступ к записям только авторизованным лицам;
- использование защищенных, генерируемых компьютером контрольных следов с указанием даты, для независимой регистрации связанных с *GxP* действий, совершенных после входа в систему[1)] .

[1)] В системах управления базами данных (СУБД) это является дополнительной функцией, однако для других приложений необходимо обеспечить ее добавление. Организацией должно быть обеспечено постоянное "включенное" состояние данной функции.

6.11 Выпуск серии

6.11.1 Если для регистрации процедуры одобрения и выпуска серии использована КС, она должна предоставлять доступ для выпуска серии только уполномоченному лицу, а также четко идентифицировать и регистрировать уполномоченное лицо, которое одобрило и выпустило серию. Эти действия следует осуществлять с использованием электронной подписи.

6.11.2 Для ведения реестра (журнала) выпущенных в обращение серий следует использовать валидированные и защищенные электронные системы обработки данных.

6.12 Непрерывность работы

6.12.1 С целью обеспечения работоспособности КС, сопровождающих критические процессы, необходимо принять меры предосторожности для гарантии непрерывности поддержки этих процессов в случае выхода системы из строя (например, с использованием ручной или альтернативной системы). Время, необходимое для введения в действие альтернативных средств, должно учитывать риски и соответствовать конкретной КС и сопровождаемому рабочему процессу. Эти меры должны быть надлежащим образом оформлены документально и проверены.

6.13 Архивирование

6.13.1 Данные могут архивироваться. Эти данные следует проверять на доступность, удобство чтения и целостность. Если в КС необходимо провести существенные изменения (например, компьютерного оборудования или ПО), должна быть обеспечена и проверена возможность восстановления данных.

Приложение А (справочное). Рекомендации по аудиту/инспектированию использования компьютеризированных систем в организации

Приложение А
(справочное)

Оценка влияния КС на соответствие требований надлежащих практик *GxP* на производственной площадке (и между производственными площадками) начинается с изучения истории работы площадки и результатов оценки рисков, проводимых на стадии подготовки к аудиту/инспекции. Порядок управления информационными технологиями, организация и проведение валидации ПО и систем на производственной площадке может контролироваться из штаб-квартиры организации. В этих случаях контроль, письменные процедуры и записи должны быть доступны для проверки на производственных площадках; в некоторых случаях может потребоваться аудит/инспектирование штаб-квартиры.

При оценке применения КС изучаются представленные организацией свидетельства о соответствии требованиям надлежащих практик КС не только в рамках технологических аспектов (например, с помощью положений руководства GAMP), но также выявленные риски в отношении несоответствия надлежащих практик *GxP* (с использованием отчетов о валидации эксплуатации и подобных документов).

Для оценки возможности критических ошибок (сбоев) КС на основании изучения интерфейсов ввода, структуры, тестов, внедрения и внесения изменений в системы рекомендуется использовать рекомендации GAMP.

Аудиторы/фармацевтические инспектора, получив четкое видение масштаба организации и сложности компьютеризации производственной площадки (или автоматизации), выборочно изучают критические системы и риски для продукции и практик *GxP*. В таблице А.1 приведен примерный опросник для сбора информации перед проведением аудита/инспекции[1)].

[1)] Для автоматизированного поиска требований в текстах документов надлежащих практик *GxP* могут быть использованы следующие ключевые слова: документ (document), спецификация (specification), регламент (formula), процедура (procedure), запись (record), данные (data), журнал (log book), инструкция (instruction), письменно/документально (written), подписывать/утверждать (sign), согласовать (approve), письменная (writing), подпись (signature), документация (documentation), авторизация/доступ (authorisation).

Таблица А.1 - Перечень информации о компьютеризированных системах, собираемых перед проведением аудита/инспекции

1 Подробное описание организации и управления ИТ/компьютерными службами и инженерными проектами на проверяемой производственной площадке
2 Политики организации по поставкам компьютерного оборудования, ПО и систем для использования в условиях надлежащих практик *GxP*
3 Политики организации в отношении валидации КС, используемых в условиях надлежащих практик *GxP*
4 Перечень стандартов и письменных процедур (стандартных операционных процедур), используемых ИТ/компьютерными службами
5 Порядок управления проектами и процедуры, применявшиеся при разработке различных приложений
6 Выявленные работы по поддержке и обслуживанию систем, передаваемые на аутсорсинг на постоянной основе
7 Перечень (реестр) всех КС, эксплуатируемых на проверяемой производственной площадке, с указанием названий и области применения и уровня бизнес-процесса, управления, информации и автоматизации. Перечень тоже должен также содержать валидационный статус и уровень риска (включая базовые схемы установленного оборудования и сетей)
8 Перечень выявленных систем, подсистем и модулей и/или программ, которые могут оказывать влияние на соответствие надлежащим практикам *GxP* и качестве продукта/безопасности пациентов. Необходимо сопоставить данный перечень с перечнями, указанными в пункте 6
9 Для критических с точки зрения *GxP* элементов и систем, выделенных в пункте 7, необходимо получить информацию, указанную в пунктах 10-17
10 Подробное описание ситуаций отказа-восстановления работы системы, резервного копирования, смены контроля, информационной безопасности и управления конфигурацией

11 Краткое описание имеющейся документации, отражающее актуальное описание систем и существующих подходов, потоков данных, взаимодействие с другими системами, записи жизненного цикла и валидации. В этом кратком описании должно быть указано, все ли из этих систем полностью документированы и валидированы, и подтверждено наличие описания критических КС
12 Информация о квалификации и обучении персонала, участвующего в разработке, кодировании, тестировании, установке и эксплуатации КС, включая консультантов и субподрядчиков [данные об образовании, стаже, описание должностных обязанностей и журналы (листы) обучения]
13 Описание используемых организацией подходов к оценке потенциальных поставщиков компьютерного оборудования, ПО и систем
14 Описание подходов, используемых организацией, по оценке наличия систем менеджмента качества и порядка валидационных работ в отношении приобретаемых или разрабатываемых самостоятельно программ
15 Описание используемых подходов к валидации и составлению документации устаревших систем, исходные записи о которых не удовлетворяют установленным требованиям
16 Сводное описание значительных изменений, сделанных с момента предыдущей инспекции/аудита и планов для будущих разработок
17 Информация о наличии и доступности записей по различным системам, их организованности; готовности ключевого персонала к представлению, обсуждению и рассмотрению подробной информации о КС, при необходимости

При отсутствии информации о компьютеризации на проверяемой площадке рекомендуется применять предынспекционный опросник для расширения информации, имеющейся в досье производственной площадки.

На основании представленной перед инспекцией информации (см. таблицы А.2, А.3, А.4, А.5, А.6) аудиторы/инспектора выбирают критические с точки зрения *GxP* КС и изучают данные о валидации этих систем, а затем результаты текущего операционного контроля о состоянии системы и ее валидности. Учитывая распределенную ответственность за *GxP*-аспекты коммерческих или бизнес ИТ-систем (различных подразделений) и процессов более низких уровней контрольных систем, следует изучить преемственность и целостность ответственности и согласованность инструкций и процедур.

Критически важным является наличие у проверяемой организации политики (порядка) проведения валидации КС, согласованной с ней письменных процедур и планов, а также перечня (реестра) всех используемых КС, классифицированных по их области применения, критичности и валидационного статуса.

Для отдельно стоящих и на протяжении длительного времени использующихся систем могла быть проведена ретроспективная валидация, а для систем, установленных после введения в действие правил надлежащих практик, должна быть проведена и документально оформлена перспективная валидация. Организация должна иметь планы по завершению любой обоснованной ретроспективной валидации КС, на которую распространены требования *GxP*, в разумные сроки с учетом рисков и сложности валидируемой системы. Продолжение использования критических систем, не поддерживаемых поставщиками и которые не могут быть валидированы, должно быть обосновано организацией, обеспечено альтернативными процедурами безопасности и управления сбоями, а также служит поводом для срочной поэтапной замены.

Подходы организации к валидации должны учитывать методологию жизненного цикла, необходимость управления контролями и документации, описанной в настоящем стандарте.

Аудиторам/инспекторам следует изучить сводный отчет о валидации[1)] в отношении выбранных для оценки систем, при необходимости, соответствующие спецификации для приемо-сдаточных испытаний системы и документацию более низкого уровня. При изучении документации следует установить наличие или отсутствие проверки критериев, установленных в соответствующих спецификациях, например:

- квалификация эксплуатации - проверка критериев спецификации требований пользователей;
- квалификация функционирования - проверка функциональной спецификации;
- квалификация монтажа - проверка спецификации проекта или обзорного проекта;
- отчеты об аудите поставщиков;
- валидационные и "квалификационные" планы, то есть основной валидационный план или политика.

[1)] Сводный валидационный план - валидационный отчет высшего уровня, в котором суммированы результаты и выводы валидационных испытаний, связанные перекрестными ссылками с отчетами более низкого уровня, подробными отчетами и протоколами. Этот документ полезен для информирования руководства организации и инспекторов регуляторных органов.

(При наличии больших валидационных работ должны быть в наличии план

качества валидационного проекта и система менеджмента качества для документации. Для небольших проектов может быть достаточным наличие документально оформленных процедур.)

При проверке следует изучить прослеживаемость действий, испытаний и устранения ошибок и отклонений в выбранной для проверки документации. При отсутствии надлежащего контроля изменений и версий системы на протяжении всего жизненного цикла и сопутствующей документации валидационный статус системы недостоверен.

Следует проверить соблюдение всех требований надлежащих практик *GxP* в выбранных для проверки валидационных проектах.

Отсутствие письменного подробного описания каждой системы (актуализируемое при помощи системы управления изменениями), функций системы, мер безопасности и взаимодействий, а также доказательств обеспечения качества процесса разработки ПО, вместе с отсутствием адекватных доказательств валидации КС, используемых в условиях *GxP*, оценивается как критическое или существенное несоответствие надлежащей практике. Значимость несоответствия оценивается аудитором/инспектором на основании оценки рисков для каждого случая.

При положительной оценке валидационной документации аудитор/инспектор изучает эксплуатацию выбранных систем с использованием распечаток отчетов системы и архивной документации, проверяя выполнение требований надлежащих практик в отношении эксплуатации КС, а также корреляцию с валидационными работами, доказательства эффективности системы управления изменениями, управления конфигурацией, правильности и надежности. В системах обработки данных обязательно анализируют порядок доступа в систему и обеспечения целостности данных.

Оценка степени значимости выявленных несоответствий основана на относительном риске приложения и оценки критичности риска несоответствия.

Таблица А.2 - Опросник аудитора/инспектора по программному обеспечению

Этап жизненного цикла	Деятельность на текущем этапе	Свидетельство
1 Разработка	Разработка спецификаций требований пользователя/функциональных спецификаций/спецификаций проекта	Документация спецификаций требований пользователя/функциональных спецификаций/спецификаций проекта
	План тестирования	План тестирования и сценарии тестирования
	Документирование плана тестирования	Письменные документы, описывающие порядок проведения тестирования
2 Внедрение	Выбор языка программирования и инструментария	Документация, описывающая выбор языка программирования
	Написание/создание ПО	Документированный исходный код с комментариями; пояснение функций; входные данные и ожидаемые выходные данные для каждого структурного модуля. Описание взаимного влияния модулей. Если программа приобретена, то каким образом гарантирован доступ к исходному коду?
3 Тестирование (модули)	Обеспечение того, что каждый модуль принимает только допустимые входные данные и выдает только допустимые выходные данные. Тестирование должно выявлять некорректные данные и логические ошибки	Образцы отчетов о тестировании (при наличии). Включало ли тестирование испытания с пограничными значениями и ввод некорректных данных? Все ли тесты были задокументированы? Все ли ошибки/сбои расследованы?

Тестирование (интегрированные модули)	Те же тесты, проведенные после интеграции модулей	Те же свидетельства. Если программа была приобретена, то доказательства валидации должны быть оценены регулируемым пользователем
4 Техническое обслуживание	Исправление ошибок, обновление версий (по необходимости)	Утвержденный порядок действий и записи, относящиеся к управлению конфигурациями и управлению изменениями. Регрессивное тестирование и периодическая оценка (в процессе внесения изменений в систему на протяжении определенного отрезка времени)
5 Документация	Системная документация (в т.ч. на ПО) корректна и актуальна	Руководства пользователей, вспомогательные СОП, правильные версии
6 Повторная валидация	Повторная валидация после внесения в программу изменений	Изменения проанализированы, решения задокументированы. Существует и описан порядок действий и записи; их масштаб зависит от размера/сложности изменений
7 Прочее	На случай сбоев в системе существуют пути их обхода; это учтено при обучении	Альтернативные пути задокументированы, существуют записи об обучении

Таблица А.3 - Опросник аудитора/инспектора по валидации компьютеризированных систем

Элемент	Проверка мер контроля
1 Описание	Система описана? Каковы ее функции? Письменный валидационный план в наличии? Имеются полные спецификации? Письменные протоколы имеются? (включая критерии приемлемости)
2 Тестирование	Записи тестов показывают соответствие спецификациям входных и выходных данных?
3 Документирование результатов	Результаты полные и документально оформлены?
4 Подтверждение правильности данных	Данные и документация полные и правильные? Были ли они проверены организацией?
5 Сопоставление с критериями приемлемости	Валидацию и проверку работ проводил компетентный ответственный персонал? Документальное подтверждение этого имеется?
6 Заключения	Заключения полные, информативные и основы* на результатах? Критерии приемлемости выполнены? Дополнительные заключения имеются?
7 Согласование (утверждение)	Согласование (утверждение) оформлено документально? Служба качества (отдел обеспечения качества/контроля качества) организации принимала участие в данной процедуре?
8 Постоянная оценка	Какая процедура существует для обеспечения постоянной оценки системы? Какие процедуры управления изменениями имеются?

---

* Текст документа соответствует оригиналу. - Примечание изготовителя базы данных.

Таблица А.4 - Опросник аудитора/инспектора по проверке требований приложения 11 надлежащей производственной практики

Номер [1]	Требование	Отметка/комментарий аудитора/инспектора
Персонал (пункт 6)	Сотрудничество между ответственным персоналом (владельцем процесса, владельцем системы, уполномоченным лицом) и ИТ-специалистами	
Персонал (пункт 6)	Персонал имеет надлежащую квалификацию, при необходимости привлекают экспертов	
Валидация (пункт 11)	Применение модели жизненного цикла, наличие документации и отчетов	
Пункт 12	Регистрация изменений и отклонений предусмотрена	
Пункт 13	Наличие актуального перечня (реестра) систем	
Пункт 14	Наличие актуального описания критических КС	
Пункт 15	Наличие спецификации требований пользователя, созданной на основании оценки рисков	
Пункт 16	КС разработана в условиях надлежащей системы управления качества	
Пункт 17	Наличие документированной процедуры оценки качества и эксплуатационных характеристик системы	

Пункт 18	Проведение тестирования согласно требованиям (пределы параметров системы, границы данных и обработка ошибок)	
	Оценка автоматизированных средств тестирования	
Пункт 19	Проверка данных в сравнении с предыдущей системой/ручным управлением	
Эксплуатация (пункт 20)	Проверка данных и расчетов, встроенных в систему	
Пункт 21	Проверка ввода критических данных вторым оператором или валидированным электронным методом	
Пункт 22	Физическая и электронная (логическая) защита данных	
Пункт 23	Наличие процедуры резервного копирования. Проведение валидации	
Пункт 24	Наличие распечаток	
Пункт 25	Проверка записи процесса разрешения на выпуск серии на предмет наличия информации о вносимых изменениях, если они были сделаны	
Пункт 26	Наличие и проверка контрольных следов	

Пункт 27	Внесение изменений в системы и программы в соответствии с процедурой управления изменениями, включая повторную валидацию и утверждения	
Пункт 28	Проведение периодической оценки, объем адекватность объема*	
Пункт 29	Осуществление ввода данных и изменения только авторизированным персоналом. Система управления паролями/ключами	
Пункт 31	Наличие записей о создании, изменении и аннулировании прав доступа	Пункт 31
Пункт 32	Система управления данными и документами для идентификации операторов и их действий с указанием дат	Пункт 32
Пункт 33	Записи показывают анализ ошибок и предпринятые корректирующие действия. Наличие отчетов о расследовании с поиском основной причины ошибки (первопричины)	Пункт 33
Пункты 34, 35	Установлены порядок применения электронных подписей и связь подписи с записями. Наличие даты и времени проставления, в том числе на записях процесса выдачи разрешения на выпуск серии в обращение	

Пункт 36	Использование альтернативных средств при сбоях предусмотрено, документально оформлено и проверено	
Пункт 37	Наличие процедуры архивирования. Подтверждение надежности процедуры восстановления данных (при изменении версии)	

_____

* Текст документа соответствует оригиналу. - Примечание изготовителя базы данных.

Таблица А.5 - Общие вопросы, рассматриваемые при аудите/инспектировании компьютеризированных систем

Раздел	Ключевой вопрос
1 Персонал	В организации одно ответственное лицо за КС? (Зависимость от одного человека может стать катастрофической)
2 Организация	Руководство участвует в управлении системами?
3 Организация	КС включены в область действия системы качества?
4 Система данных	В начале инспекции изучают общую организацию систем, включая потоки данных?
5 Система данных	Использование "параллельных систем" может свидетельствовать о наличии "серых" зон и вероятности несоответствия систем требованиям
6 Валидация	Определения четко сформулированы? Их использование корректно?
7 Безопасность	Как контролируют доступ к системам? Оценка системы управления информационной безопасностью
8 Техническое обслуживание	Наличие руководства по техническому обслуживанию каждой системы с указанием периодичности обслуживания. Наличие соответствующих записей о выполнении данного руководства
9 Контроль системы	Процедуры управления конфигурацией, управление изменениями
10 Самоинспекции	Наличие процедуры самоинспекции и ее проведение

Таблица А.6 - Основные обязанности организации-пользователя (согласно руководству GAMP, см. также 4.6)

Задача	Описание
1 Идентификация системы	Должна быть оценена каждая автоматизированная система и определены системы, подпадающие под требования надлежащих практик *GxP*
2 Разработка спецификаций требований пользователя	В спецификациях требований пользователя должно быть четко и однозначно указано, что ожидает пользователь от системы (что она должна делать). Должны быть указаны любые ограничения, а также определены регуляторные и документальные требования
3 Определение валидационной стратегии	
Оценка рисков	Исходная оценка рисков должна быть проведена на этапе планирования валидации. В дальнейшем оценки должны производить по мере разработки спецификаций
Оценка компонентов системы	Компоненты системы должны быть оценены и разбиты на категории с целью определения требуемого валидационного подхода. Выходные данные этого процесса лягут в основу плана валидации
Оценка поставщика	Поставщики должны быть формально оценены в рамках процесса выбора поставщика и планирования валидации. Необходимость проведения аудита поставщика (или исключения данным этапом) должна быть задокументирована и основана на оценке рисков и категоризации компонентов системы
4 Разработка плана валидации	В плане валидации должны быть указаны действия, процедуры, направленные на подтверждение пригодности системы, и степень ответственности. В плане обычно указывают, какие оценки рисков необходимо осуществлять
5 Анализ и утверждение спецификаций, в т.ч. описания системы	Организация должна проанализировать и утвердить спецификации, разработанные поставщиком

6 Мониторинг разработки системы	Организация должна мониторировать разработку и конфигурирование в соответствии с согласованным планом
7 Анализ исходного кода	Организация должна обеспечить адекватный анализ исходного кода в процессе разработки системы
8 Анализ и утверждение спецификаций тестирования	Организация должна проанализировать и утвердить спецификации до начала официального тестирования
9 Проведение тестирования	Организация может участвовать в тестировании в качестве наблюдателя или рецензента результатов тестирования
10 Анализ и утверждение отчетов о тестировании	Организация должна утвердить отчеты о тестировании и соответствующие результаты тестирования
11 Создание валидационного отчета	В валидационном отчете должны быть приведены все результаты и действия, а также свидетельства того, что система валидирована
12 Обслуживание системы	После принятия системы организация должна разработать надлежащие принципы системного администрирования и производственной деятельности
13 Прекращение эксплуатации	Организация должна управлять процессом замены или выведения автоматизированной системы из эксплуатации

Библиография

[1] Приказ Минпромторга России от 14 июня 2013 N 916 (ред. от 18 декабря 2015) "Об утверждении Правил надлежащей производственной практики"

[2] Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"

[3] EU Annex 11 to the EU guidelines of Good Manufacturing Practice for Medicinal Products

[4] Annex 11 to PIC/S Guide to Good Manufacturing Practice for Medicinal Products, Document PH 1/97 (Rev. 3), PIC/S Secretariat, 9-11 rue de Varembé, CH-1211 Geneva 20

[5] IEEE 1298 Software quality management system; part 1: requirements

[6] IEEE 829 Standard for software test documentation

УДК 004.9:006.354 ОКС 13.060.70

Ключевые слова: компьютеризованные системы, лекарственные средства, правила надлежащей производственной практики, правила надлежащей дистрибьюторской практики, надлежащая лабораторная практика

Электронный текст документа
подготовлен АО "Кодекс" и сверен по:
официальное издание
М.: Стандартинформ, 2019