ПРИЛОЖЕНИЕ

к Рекомендации Коллегии
Евразийской экономической комиссии
от 20 г. №

Р У К О В О Д С Т В О
по обеспечению целостности данных и валидации компьютеризированных систем

I. Общие положения

1. В целях обеспечения безопасности пациентов и качества лекарственной продукции Решением Совета Евразийской экономической комиссии от 3 ноября 2016 г. № 77 утверждены Правила надлежащей производственной практики Евразийского экономического союза (далее соответственно – Правила GMP, GMP). Правила GMP устанавливают требования к организации производства и контроля качества лекарственных средств для медицинского применения и ветеринарных лекарственных средств, позволяя гарантировать высокое качество выпускаемой продукции сохраняющееся от серии к серии. Принятие решений о выпуске продукции уполномоченным лицом по качеству основывается на управляемых данных, создаваемых и поддерживаемых как единое целое в течение всего жизненного цикла продукции так, чтобы существовала возможность проследить все предпринятые действия в отношении такой продукции.

2. Управление данными обеспечивается благодаря продолжающемуся развитию вспомогательных технологий (таких, как использование электронного сбора данных, автоматизация систем и использование дистанционных технологий) и связано с непрерывно возрастающей сложностью цепи поставок и способов работы (например, через поставщиков услуг). Системы, поддерживающие эти методы работы, могут использовать как ручные процессы с бумажными записями, так и полностью компьютеризированные системы.

3. В приложении № 11 к Правилам GMP определяются требования к критическим записям в системе GMP, управляемым с помощью компьютеризированных систем. Данные требования включают в себя обеспечение целостности данных, управляемых с помощью автоматизированных систем.

4. Принципы целостности данных в равной степени применимы как к не компьютеризированным, так и компьютеризированным системам и не должны ограничивать разработку или внедрение новых концепций или технологий.

5. Целостность данных определяется как «степень полноты, последовательности и точности данных на протяжении всего жизненного цикла данных», и имеет основополагающее значение в фармацевтической системе качества, которая обеспечивает необходимое качество лекарственных средств. Ненадлежащие методы обеспечения целостности данных и их уязвимость подрывают качество записей и в конечном счете могут компрометировать качество лекарственных средств.

6. Целостность данных применима ко всем элементам системы управления качеством, и изложенные в настоящем документе принципы в равной степени применимы к данным, получаемым с помощью

электронных и бумажных систем; эти данные должны оцениваться на предмет выявления потенциальной уязвимости и принятия мер по разработке и внедрению надлежащей практики управления данными в целях обеспечения их целостности.

7. Меры, рассматриваемые в настоящем руководстве, ориентированы на то, чтобы обеспечить эффективность инспекционных процессов оценки соответствия фармацевтических производителей требованиям надлежащей производственной практики, основанную на достоверности предоставляемых документов, и в конечном счете, на целостности исходных данных. Для инспекционного процесса крайне важно, чтобы инспекторы могли определять и в полной мере полагаться на точность и полноту представляемых им доказательств и документации.

8. Настоящее Руководство направлено на использование риск-ориентированного подхода к управлению данными, который включает риск, критичность и жизненный цикл данных. Пользователям настоящего Руководства необходимо понимать управление данными (как жизненный цикл), чтобы идентифицировать данные, оказывающие наибольшее влияние на процессы GMP. Исходя из этого, можно определить и внедрить наиболее эффективный и действенный контроль, основанный на оценке рисков, и обзор данных.

9. Рекомендации и методы, приведенные в данном руководстве, подготовлены на основе аналогичных руководств международных и региональных организаций (Системы сотрудничества фармацевтических инспекций (PIC/S), Всемирной организации здравоохранения (ВОЗ), Управления по контролю лекарственных средств и изделий медицинского назначения Великобритании (MHRA), Международного общества по фармацевтическому инжинирингу

(ISPE), Ассоциации производителей лекарственных средств для парентерального применения (PDA)).

10. Настоящее Руководство не описывает каждый возможный сценарий обеспечения целостности данных, поэтому в тех случаях, когда применяемый подход отличается от описанного в данном документе, следует руководствоваться принципами изложенными в документах организаций, перечисленных в пункте 9 настоящего Руководства, либо обращаться за консультацией в соответствующие уполномоченные органы.

II. Сфера применения

11. Настоящее Руководство позволяет сформировать систему, объединяющую рациональную организационную практику, эффективные процессы, основанные на оценке рисков, и соблюдение требований права Союза для обеспечения целостности тех записей, которые могут оказать потенциальное влияние на безопасность пациентов и качество продукции.

12. Поскольку целостность данных применима ко всем элементам системы управления качеством, руководство содержит указания в части обеспечения целостности важнейших записей, фиксация и управление которыми происходит как с помощью бумажных носителей, так и компьютеризированных систем, и проведения (осуществления) валидации компьютеризированных систем, что является ключевым требованием для обеспечения целостности записей.

13. Цели настоящего Руководства:

представление указаний по проверке обеспечения целостности данных на соответствие требованиям Правил GMP;

представление консолидированных, наглядных рекомендаций фармацевтическим производителям и другим участникам системы обращения лекарственных средств по риск-ориентированным стратегиям контроля, которые позволяют реализовать критически важные указания по обеспечению целостности и надежности данных в контексте современных отраслевых практик и глобализованных цепей поставок;

обеспечение эффективного внедрения элементов целостности данных в планирование и проведение процесса квалификации GMP-критичных поставщиков;

определение процедурной базы, соответствующей нормативным требованиям к управлению компьютеризированными системами, изложенным в приложении № 11 к Правилам производственной практики.

14. Положения настоящего Руководства применяются к записям, генерируемым, поддерживаемым в рабочем состоянии и (или) хранимым вручную или электронным способом, от создания до архивирования, для поддержания процессов GMP, используемых фармацевтическими компаниями для гарантии высокого качества производимой продукции от серии к серии.

15. Подходы к обеспечению целостности данных, изложенные в настоящем руководстве, применимы в равной степени к бумажным и электронным данным, генерируемым или используемым в рамках любого процесса, способного оказать потенциальное воздействие на безопасность пациентов и качество продукции на различных этапах ее производства и дистрибуции.

16. В случае передачи одного из критических процессов на аутсорсинг, организация, передающая работу, несет ответственность за

целостность всех сообщаемых результатов, включая результаты, представленные любой аутсорсинговой организацией или поставщиком услуг (в соответствии с разделом VIII настоящего Руководства).

17. В случае если регламентирующие данные создаются, управляются и ведутся с помощью электронных записей, связанная с этим целостность обеспечивается соответствующей компьютеризированной системой. Положения настоящего Руководства применяется ко всем компьютеризированным системам, способным оказать влияние на выполнение требований Правил GMP, которые потенциально могут повлиять на безопасность пациента и качество продукции.

18. Руководство может быть на добровольной основе использовано в иных сферах надлежащих практик (GxP): дистрибьюторской, клинической, лабораторной и надлежащей практики фармаконадзора, а также в иных смежных сферах процесса обращения лекарственных средств (например, в деятельности лабораторий по контролю качества лекарственных средств).

19. Для целей настоящего Руководства используются понятия, которые означают следующее:

«валидация компьютеризированных систем» – подтверждение посредством оценки и предоставления объективных доказательств того, что характеристики компьютеризированной системы соответствуют потребностям пользователя и своему назначению, а все требования стабильно выполняются;

«данные» – информация, извлеченная или полученная из исходных данных (например, зарегистрированный аналитический результат), которая соответствует критериям «ALCOA+»;

«динамическая запись» – записи в динамическом формате, такие как электронные записи, которые обеспечивают интерактивную связь между пользователем и содержимым записи (к таким записям относятся в том числе электронные записи в форматах баз данных, которые позволяют проследить, оценить тренды и запросить соответствующие данные; результаты хроматографии, хранящиеся в электронном виде, которые позволяют пользователю выполнить повторную обработку данных, просмотреть скрытые поля при наличии соответствующих прав доступа, а также изменять отображение основной линии хроматограммы для более четкого обзора результатов интегрирования хроматографических пиков);

«жизненный цикл данных» – цикл, охватывающий все этапы существования данных (включая необработанные данные), начиная с их создания и записи, обработки (включая преобразование или миграцию), использование, хранение, архивирование (извлечение) и заканчивая уничтожением данных;

«истинная копия» – точная копия исходной информации, имеющая атрибуты и информацию исходной записи и сохраняющая целостность, точность, полное содержание, форматы дат, электронную подпись, разрешения и полный контрольный след;

«исходная запись» – данные в виде файла или формата, в котором они были первоначально созданы, с сохранением целостности (точности, полноты, содержания и значения) записи (например, оригинальная бумажная запись, полученная вручную или электронный файл необработанных данных из компьютеризированной системы) и позволяют полностью реконструировать деятельность, приводящую к получению данных;

«компьютеризированная система» – система, коллективно контролирующая выполнение одного или нескольких автоматизированных бизнес-процессов и включающая в себя компьютерное оборудование, программное обеспечение, периферийные устройства, сети (при наличии), персонал и документацию (например, руководства, стандартные операционные процедуры);

«контрольный след» – процесс, который фиксирует такие детали, как добавления, удаления или изменения информации в записи в бумажной и электронной форме, без затенения или переписывания исходной записи и облегчает восстановление истории подобных событий, связанных с записью, независимо от носителя, включая информацию, о каждом действии относительно его автора, вида действия, времени и причины совершения («кто, что, когда и почему»);

«метаданные» – данные, являющиеся неотъемлемой частью исходной записи, которые описывают свойства других данных (как правило, структуру, элементы данных, взаимосвязи и другие характеристики данных), формируя их специфические признаки и смысловое содержание, а также позволяя соотнести данные с отдельным лицом или, если они генерируются автоматически, конкретным источником данных. Данные, лишенные метаданных рассматриваются как бессмысленные;

«обзор данных» – процедура, описывающая процесс обзора и утверждения данных, которая включат в себя в том числе и обобщение соответствующих метаданных (то есть контрольный след), а также действия, которые должны быть предприняты, если анализ данных выявит ошибку или какое-либо упущение;

«обработка данных» – последовательность операций, выполняемых с данными с целью извлечения, представления или

получения информации в определенном формате (например, статистический анализ для ежегодного обзора продукции);

«первичная запись» – запись, которая имеет преимущественную силу в тех случаях, когда данные, которые собираются и хранятся одновременно более чем одним методом, не совпадают между собой;

«полное время обработки образцов» – временной период между созданием (отбором) образцов и завершением их анализа (то есть время, необходимое для завершения всех анализов для данной серии образцов);

«регулируемые данные – данные, используемые в сфере GMP, требуемые Правилами GMP и относящиеся к действиям, которые могут повлиять на безопасность пациента и качество продукции;

«регулируемая компания» – фармацевтическая компания, которую требуется оценить на соответствие Правилам производственной практики в соответствии с актами органов Союза в сфере обращения лекарственных средств или в связи с иными бизнес-причинами;

«статическая запись» – документ с фиксированными данными (например, бумажная запись или электронное изображение) (к статическим записям относятся в том числе список записей по обучению или статическое изображение, созданное во время сбора данных).

III. Концепция обеспечения целостности данных

1. Понятие «целостность данных» и принципы обеспечения целостности данных

20. Уполномоченные органы при проведении оценки целостности данных принимают во внимание научные теоретические наработки и опыт организаций, которые разрабатывают, производят и упаковывают,

тестируют, распространяют и контролируют фармацевтическую продукцию. В процессе оценки и анализа подразумевается взаимное доверие между уполномоченным органом и фармацевтической компанией, участвующей в системе обращения лекарственных средств, относительно всестороннего, полного и надежного представления используемой в процессе принятия решений информации (данных) в регистрационном досье лекарственного препарата.

21. Меры контроля для обеспечения целостности данных встраиваются в фармацевтическую систему качества, которая гарантирует, что лекарственные средства имеют требуемое качество. Целостность данных применима ко всем элементам фармацевтической системы качества, и принципы, изложенные в настоящем Руководстве, в равной степени применимы к данным, создаваемым электронными и бумажными системами. Для обеспечения точности, полноты, последовательности и надежности записей и данных на протяжении всего периода их востребованности (то есть на протяжении всего жизненного цикла данных) организации должны следовать надлежащей практике документирования (GDocP).

22. Усилия и ресурсы, направляемые регулируемой компанией на контроль целостности данных, следует соизмерять с риском для качества продукции, а также сопоставлять с другими запросами ресурсов обеспечения качества. Фармацевтическим компаниям следует разработать и использовать методическую базу, которая обеспечит приемлемое контролируемое состояние, основанное на оценке рисков целостности данных. Методическую базу следует полностью документировать с соответствующим логическим обоснованием.

23. Ответственность за надлежащую практику в отношении управления данными и их целостности лежит на производителе,

проходящем проверку. Производитель несет полную ответственность и обязан оценивать свои системы управления данными на предмет потенциальных уязвимостей и принимать меры по разработке и внедрению надлежащей практики управления данными для обеспечения сохранения целостности данных.

24. Руководство регулируемой компании несет главную ответственность за распределение ресурсов и осуществление мер контроля, направленных на сведение к минимуму потенциального риска для целостности данных, а также за идентификацию остаточного риска.

25. Регулируемые компании несут ответственность за используемые ими системы и данные, генерируемые этими системами. В компании должна существовать культура, обеспечивающая полноту, целостность и точность данных во всех формах (в бумажной и электронной). Каждого оператора, занятого сбором, представлением или поддержанием данных, должен быть надлежащим образом проинформирован об ожиданиях целостности данных и находиться под постоянным контролем.

26. Заинтересованные стороны, передавшие на аутсорсинг третьей стороне процессы, которые могут оказать влияние на результаты клинических исследований, производство, контроль качества или дистрибуцию, несут ответственность за соответствие третьей стороны положениям настоящего Руководства.

2. Применение критериев «ALCOA+» при оценке данных

27. Для обеспечения качественной информированности о процессе принятия решений и для подтверждения достоверности информации, события или действия, послужившие основанием для принятия этих

решений, следует надлежащим образом задокументировать. Надлежащая практика документирования (GDocP) являются ключом к обеспечению целостности данных и важной частью фармацевтической системы качества. Применение надлежащей практики документирования (GDocP) может варьироваться в зависимости от носителя, используемого для записи данных (физические носители информации или электронные носители информации), но принципы применимы к обоим носителям.

Данные, на которых основаны любые решения, должны соответствовать критериям «ALCOA+», которые включают в себя:

прослеживаемость (A – attributable) данных до лица, создавшего запись;

читаемость (L – legible) данных,

своевременность (C – contemporaneous) данных,

подлинность (O – original) данных

точность (A – accurate) данных;

соответствие дополнительным требованиям, обеспечивающим полноту (complete), последовательность (consistent), устойчивость (enduring) и доступность (available) данных (обозначенных в акрониме символом «+»).

28. Выполнение всех критериев ALCOA+ гарантирует, что события должным образом задокументированы и данные могут использоваться для принятия обоснованных решений. В совокупности эти критерии направлены на обеспечение точности информации, в том числе научных данных, которые используются для принятия критических решений о качестве продукции. В целях подтверждения выполнения критериев ALCOA+ следует:

а) для прослеживаемости – обеспечить идентификацию лица, и (или) компьютеризированной системы, выполнивших записанное задание. Следует документировать, кто выполнил задачу и (или) функцию, подтвердить, что задача и (или) функция были выполнены обученным и квалифицированным персоналом. Это также касается любых изменений, внесенных в записи (исправлений, удалений, изменений и т. д.);

б) для читаемости – обеспечить, чтобы все записи были разборчивыми, а информация была читаема в течение всего периода хранения. Это относится ко всей информации, которая будет считаться полной, включая все исходные записи или заметки. В тех случаях, когда динамический характер электронных данных важен для содержания и смысла записи, возможность работать с данными с помощью подходящего приложения следует обеспечить в течение периода хранения (то есть данные сохраняются в электронном формате, который позволяет к ним обращаться и обрабатывать);

в) для своевременности – обеспечить, чтобы доказательства действий, событий или решений регистрировались по мере их совершения. Эта регистрирующая документация служить точным подтверждением того, что и по какой причине было сделано или решено (что повлияло на принятие решения в соответствующий период времени);

г) для подлинности – подлинную запись определять как первую записанную информацию, в бумажном (статическая информация) или в электронном виде (обычно динамическая информация, в зависимости от сложности системы). Информация, первоначально захваченная в динамическом состоянии, должна оставаться доступной в этом состоянии;

д) для точности – обеспечение точности сведений и записей за счет применения множественных элементов устойчивой фармацевтической системы качества может основываться на:

факторах, связанных с оборудованием (например, квалификация, калибровка, техническое обслуживание и валидация компьютеризированных систем);

политике и процедурах контроля действий и поведения персонала;

процессах оценки данных на предмет соблюдения процедурных требований;

управлении отклонениями, включая анализ исходных причин, оценку воздействия и план корректирующих и предупреждающих действий (CAPA);

обученном и квалифицированном персонале, понимающем важность соблюдения установленных процедур и документирования своих действий и решений;

е) для полноты – подтвердить, что вся необходимая (критическая) информация для воссоздания интересующего события, является достаточной и надлежащей. Уровень детализации, необходимый для того, чтобы набор информации считался полным, будет зависеть от критичности информации. Полная запись данных, полученных в электронном виде, включает в себя соответствующие метаданные;

ж) для последовательности – обеспечить, чтобы надлежащая практика документирования применялась на протяжении всего процесса работы с данными без исключений, включая отклонения и изменения, которые могут произойти в ходе процесса;

з) для устойчивости – предусмотреть, чтобы частью обеспечения доступности данных являлось обеспечение их существования в течение всего периода, в течение которого они могут потребоваться. Данные

должны оставаться нетронутыми и доступными в неудаляемом (надежном) формате;

и) для доступности – обеспечить, чтобы записи были доступны для рассмотрения в любое время в течение требуемого периода хранения для рутинных решений о выпуске, расследований, трендов, годовых отчетов, аудитов или инспекций. Записи должны быть доступны в формате, удобном для чтения персоналу, ответственному за их рассмотрение.

IV. Средства обеспечения целостности данных

1. Система управления данными

29. Управление данными – это совокупность организационных мероприятий, обеспечивающих целостность данных. Управление данными обеспечивает полноту, последовательность и точность записи на протяжении всего жизненного цикла данных, независимо от процесса, формата или технологии, в которых они генерируются, регистрируются, обрабатываются, сохраняются, извлекаются и используются.

В процессе управления данными выполнение обзора данных основывается на исходных данных или их точной копии и документируется. Обзор данных должен позволять вносить исправления или уточнения в данные в соответствии с Правилами производственной практики, обеспечивая читаемость исходной записи и прослеживаемость исправления с использованием критериев ALCOA+

30. Управление данными распространяется на владение данными и подотчетность на протяжении всего жизненного цикла данных, проектирования, использования и мониторинга процессов и (или)

систем в соответствии с принципами целостности данных, включая контроль за преднамеренными и непреднамеренными изменениями данных.

Следует обеспечить прослеживаемость любого заранее определенного параметра, используемого в деятельности по обработке данных. Контрольный след и сохранность записи должны позволять реконструкцию всех действий по обработке данных независимо от того, включается ли итог обработки в последующий отчет или используется иначе. Если обработка данных повторяется с постепенным изменением параметров обработки, то это следует зафиксировать для обеспечения отсутствия манипуляций параметрами обработки в целях достижения желаемых конечных данных.

Следует также надлежащим образом определить полное время обработки образцов при формировании данных (записей) о результатах анализов, поскольку, если этот период будет необоснованно коротким, персонал вынужден будет нарушать целостность данных для того, чтобы обеспечить их кажущееся соответствие ожидаемому периоду времени обработки образцов.

31. Системы управления данными являются неотъемлемой частью фармацевтической системы качества (PQS) для каждого этапа жизненного цикла продукции. Фармацевтическая система качества должна располагать данными, полученными на протяжении всего жизненного цикла продукции и учитывать проектирование, использование и мониторинг процессов и (или) систем в целях соблюдения принципов целостности данных, включая контроль преднамеренных и непреднамеренных изменений и удаления информации.

32. Эффективная система управления данными подразумевает со стороны руководства регулируемой компании внедрение и последовательное соблюдение надежных практик управления данными, в том числе и в отношении:

а) соответствующей организационной (корпоративной) культуры компании и моделей поведения;

б) понимания риска, связанного с обеспечением целостности данных на протяжении их жизненного цикла.

33. Указания по обеспечению целостности данных доводятся до сведения персонала всех уровней в документарной форме. Следует поощрять открытое (свободное) информирование соответствующих ответственных лиц о нарушениях, наблюдаемых операторами компании. Сотрудники компании могут рекомендовать улучшения, направленные на предотвращение фальсификации данных. Это снижает риск фальсификации, изменения или удаления данных.

34. Системы управления данными включают в себя подготовку персонала в отношение важности принципов целостности данных и создания рабочей среды, которая обеспечивает выявление и поощряет активное предоставление информации об ошибках, упущениях и нежелательных результатах.

35. Степень знания и понимания руководством регулируемой компании целостности данных может повлиять на успех компании в управлении целостностью данных. Руководство регулируемой компании должно располагать достаточными знаниями и полномочиями для предотвращения нарушений целостности данных и иметь возможность их обнаружения, если такие нарушения целостности данных происходят.

2. Риск-ориентированный подход к управлению данными

36. Управление рисками для качества (QRM) имеет важное значение для эффективной программы управления данными. Усилия и ресурсы, выделяемые на управление данными и записями, следует соизмерять с риском: подход к управлению записями и данными, основанный на оценке рисков, призван обеспечить уверенность в том, что для обеспечения целостности данных, относящихся к сфере GMP, выделены достаточные ресурсы и применяются необходимые стратегии контроля.

37. Поскольку не все этапы обработки данных имеют одинаковое значение для качества продукции и безопасности пациентов, для определения важности каждого этапа обработки данных следует использовать управление рисками для данных. Эффективный подход к управлению данными основан на оценке риска для целостности данных, определяемом следующими факторами:

а) критичность данных (влияние на принятие решений и качество продукции);

б) подверженность данных нарушениям (возможность изменения и удаления данных, а также вероятность обнаружения (выявляемость) изменений в процессе рутинной проверки со стороны производителя). Подверженность данных нарушениям определяется потенциальной возможностью удаления, изменения или исключения данных незарегистрированным лицом и возможностью обнаружения таких действий и событий.

38. Риски для данных могут возрастать в результате сложных, непоследовательных процессов с открытыми и субъективными результатами по сравнению с простыми задачами, которые

выполняются последовательно, надлежащим способом определены и имеют четкую цель.

39. Сокращение усилий и (или) частоты контрольных мер может быть оправдано для данных, которые оказывают меньшее воздействие на продукцию, безопасность пациента или рабочую среду; если эти данные получены в процессе, который не дает возможности для внесения изменений без доступа к системе высокого уровня или специализированного программного обеспечения (специальных знаний).

40. Организации должны разработать, внедрить и эксплуатировать документированную систему, обеспечивающую приемлемое состояние контроля на основе риск-ориентированного подхода к управлению целостностью данных с соответствующим обоснованием. Примером приемлемого подхода является оценка риска целостности данных (data integrity risk assessment (DIRA)), при которой процессы, производящие данные, или в результате которых получены данные, картируются, критические воздействия идентифицируются, а присущие риски документируются.

41. Оценку рисков следует ориентировать на конкретный процесс (например, производство, контроль качества). Следует оценивать потоки данных и методы получения данных, а не просто учитывать функциональность или сложность компьютеризированной системы. Факторы для рассмотрения включают в себя:

а) сложность процесса;

б) методы генерирования, хранения и удаления данных и их способность обеспечивать точность, удобочитаемость, неудаляемость данных;

в) последовательность процессов и степень автоматизации и (или) человеческий фактор;

г) субъективность результата (является процесс открытым или четко определенным);

д) результаты сопоставления данных электронной системы и событий, зарегистрированных вручную, могут быть показательными для выявления нарушений (например, явных расхождений между аналитическими отчетами и временем сбора необработанных данных).

3. Жизненный цикл данных

42. Жизненный цикл данных распространяется на то, как данные генерируются, обрабатываются, сообщаются, проверяются, используются для принятия решений, а также хранятся (архивируются) и окончательно удаляются (уничтожаются) в конце срока хранения. Процедуры уничтожения данных учитывают критичность данных и, при необходимости, требования законодательства государства – члена Евразийского экономического союза в отношение их хранения. Архивационные меры принимаются для долгосрочного хранения соответствующих данных в соответствии с законодательством государства – члена Евразийского экономического союза.

Данные, относящиеся к продукту или процессу, могут пересекать различные границы в течение жизненного цикла. Это может включать передачу данных между ручными и IT-системами или между различными организационными границами, как внутренними (например, между производством, контролем качества и обеспечением качества), так и внешними (например, между поставщиками услуг или подрядчиками и заказчиками).

43. Управление данными следует применять на протяжении всего жизненного цикла данных для обеспечения целостности данных. Данные могут храниться в исходной системе при условии соответствующего контроля либо в организованном архиве. Данные по способу их записи могут быть:

а) бумажными – в виде бумажной записи о наблюдении или деятельности, сделанной вручную. Бумажные записи могут потребовать независимой проверки, если это будет сочтено необходимым согласно оценке риска целостности данных, или согласно иному требованию актов права Союза в сфере обращения лекарственных средств. Следует учитывать меры по снижению риска, особенно в отношении данных, связанных с высокой критичностью;

б) электронными – в виде электронной записи, получаемой при использовании как простого оборудования, так и сложных компьютеризированных систем. Присущий риск для целостности данных, связанный с оборудованием и компьютеризированными системами, может различаться в зависимости от того, в какой степени система (генерирующая или использующая данные) может быть сконфигурирована, а также от возможности манипулирования данными во время передачи между компьютеризированными системами в течение жизненного цикла данных. Следует расширять использование имеющихся технологий, надлежащим образом сконфигурированных для снижения риска нарушения целостности данных. Простые электронные системы, не имеющие программной настройки и средств электронного хранения данных (например, pH-метры, весы и термометры) могут потребовать только калибровки и (или) поверки. В то же время сложные электронные системы требуют «валидации по назначению» (в соответствии с пунктами 108 – 110 настоящего Руководства).

В любом случае тщательная оценка электронной системы записей является обязательной, поскольку все системы, упомянутые в качестве примеров, могут иметь очень сложную структуру. Важно не упускать из виду системы меньшей сложности, например, отдельно стоящие системы с пользовательскими настройками (такие как электрокардиографы, ИК Фурье-спектрометры и УФ-спектрофотометры), поскольку данными этих систем возможно манипулировать или повторять измерение с их использованием для достижения желаемого результата, с лимитированной возможностью обнаружения указанного;

в) гибридными – при которых исходную запись формируют как бумажные, так и электронные записи. При использовании гибридных систем записи данных следует четко определить первичные записи (все доказательства следует рассмотреть и сохранить). Гибридные системы следует сконструировать таким образом, чтобы они отвечали желаемой цели;

г) прочими – полученными с использованием иных систем записи и представляющими собой фотографии, иные способы фиксации изображения и хроматографические пластины. Если полученные данные записываются с помощью фотографии или иной фиксации изображения, или с помощью другого носителя, то для выбора условий хранения такого формата данных на протяжении всего их жизненного цикла следует руководствуются теми же соображениями, что и для других форматов данных, учитывая любые дополнительные элементы, необходимые для указанного формата.

44. Необработанные данные определяются как исходная запись (данные), которая может быть описана как первая запись информации в бумажном носителе или в электронном виде.

45. Независимо от формата записи (бумажный или электронный), необработанные данные должны соответствовать критериям ALCOA+. Информация, первоначально записанная как динамическая, должна оставаться доступной в этом состоянии.

46. Необработанные данные должны позволять полностью реконструировать порядок предпринятых действий.

47. Если были получены динамические данные, то бумажные копии не могут рассматриваться как необработанные данные. В случае, если технические ограничения не позволяют сохранить динамическую природу записей, доступные варианты хранения данных следует оценивать с учетом риска и важности данных с течением времени. Рекомендации по архивированию данных приведены в пунктах 134 – 138 настоящего Руководства.

48. В случае если основное электронное оборудование не имеет возможности хранить электронные данные или обеспечивает только печатный вывод данных (например, весы или pH-метры), полученные с них распечатки представляют собой необработанные данные. В случаях, когда основное электронное оборудование хранит электронные данные на постоянной основе, но способно хранить только определенный ограниченный объем данных до их перезаписи, указанные данные должны периодически просматриваться и, при необходимости, сверяться с бумажными записями и извлекаться в качестве электронных данных, если это поддерживается самим оборудованием. Критерии ALCOA + применяются также к метаданным.

4. Факторы, связанные с работой регулируемой компании

Организационная (корпоративная) культура компании

49. Следует уделять большое внимание организационной (корпоративной) культуре компании, показателям эффективности, целям и мотивации персонала компании на достижение успешности мер управления данными, заданными высшим руководством регулируемой компании. Политика управления данными (или ее эквивалент) утверждается высшим руководством регулируемой компании.

50. Руководству регулируемой компании следует сформировать прозрачную и открытую рабочую среду (организационную (корпоративную) культуру компании), в которой персонал компании может свободно сообщать о сбоях и ошибках процессов, включая потенциальные проблемы с надежностью данных, с тем чтобы можно было проводить соответствующие корректирующие и предупреждающие мероприятия.

51. Структура организационной подчиненности должна обеспечивать информационный поток между сотрудниками всех уровней. Эффективному управлению данными в одних случаях может способствовать расширение прав и возможностей сотрудников для выявления и сообщения о проблемах посредством системы качества. В других случаях для достижения эквивалентного уровня контроля может потребоваться большее внимания надзору и вторичной проверке в связи с социальным барьером на пути передачи нежелательной информации.

52. Возможность прямого анонимного обращения к руководству может также быть важной в этой ситуации.

53. Руководство регулируемой компании может стимулировать внедрение и развитие организационной (корпоративной) культуры компании посредством:

обеспечения осведомленности персонала компании и понимания персоналом ожиданий компании относительно своего персонала (например, путем принятия Кодекса этики компании и Кодекса поведения персонала компании или аналогичных им документов);

лидерства посредством личного примера, посредством которого руководство должно демонстрировать то поведение, которое оно ожидают увидеть от подчиненных;

обеспечения отчетности за действия и решения;

постоянного и активного участия;

установления реалистичных ожиданий с учетом ограничений, которые оказывают давление на сотрудников.

Кодекс этики компании и Кодекс поведения персонала компании

54. Кодекс этики компании должен отражать философию руководства компании в отношении качества работ и продукции, достигаемых посредством моделей поведения (то есть Кодекса поведения персонала компании), которые соответствуют организационной (корпоративной) культуре компании и создают атмосферу доверия, в которой все сотрудники несут ответственность за обеспечение безопасности пациентов и качества продукции.

55. Общие стандарты этики и добросовестного поведения персонала компании должны быть установлены и известны каждому сотруднику компании, и соответствующие ожидания руководства

компании должны доводиться до сведения персонала своевременно и на регулярной основе.

56. Политики Кодекса поведения персонала компании должны четко определять нормы этического поведения, такие как честность. Это должно быть доведено до сведения всего персонала и должно быть надлежащим образом понято. Недостаточно ограничиваться только знанием требований, следует понимать также то, почему требования были установлены, и последствия их невыполнения. В отношении нежелательных действий (например, преднамеренной фальсификации данных, несанкционированных изменений, уничтожения данных или других действия, нарушающих целостность данных), следует принять незамедлительные меры. При необходимости принимаются дисциплинарные меры; в то же время, поведение, соответствующее требованиям, следует определить надлежащим образом.

Программы обучения

57. Персонал следует обучить политике целостности данных и ее соблюдению. Руководству компании следует обеспечить, чтобы персонал был обучен понимать разницу между надлежащим и ненадлежащим поведением в политике целостности данных и выявлять ненадлежащее поведение (включая преднамеренную фальсификацию), а также был осведомлен о потенциальных последствиях ненадлежащего поведения.

58. Ключевых сотрудников, включая управленческий персонал, руководителей и работников службы качества, следует обучить мерам по предотвращению правонарушений и обнаружению подозрительных данных.

59. Руководству регулируемой компании также следует обеспечить обучение всего персонала процедурам обеспечения надлежащей практики документирования (GDocP) (как для бумажных, так и для электронных записей) как при наборе персонала, так и периодически в процессе трудовой деятельности (по мере необходимости).

Совершенствование фармацевтической системы качества

60. Применение современных принципов управления рисками для качества и надлежащей практики управления данными к существующей фармацевтической системе качества служит для модернизации системы качества в целях решения задач, которые возникают в связи с генерацией сложных данных.

61. Фармацевтическая система качества компании должна быть способна предотвращать, обнаруживать и исправлять слабые места в системе или процессах, которые могут привести к нарушениям целостности данных. Компания должна знать жизненный цикл своих данных и интегрировать соответствующие средства контроля и процедуры, чтобы полученные данные были пригодными, полными и надежными. В частности, такой контроль и соответствующие процедурные обновления могут осуществляться в следующих областях:

а) оценка и управление рисками;

б) программы расследований, направленные на предотвращение нарушений целостности данных и (или) на изучение выявленных нарушений;

в) практика обзора данных;

г) валидация программного обеспечения;

д) управление поставщиками (подрядчиками);

е) программа обучения, включающая политику целостности данных и процедуры по целостности данных;

ж) включение принципов обеспечения целостности данных в программу самоинспекции.

Показатели качества и отчетность перед высшим руководством

62. Следует критически осмыслять эффективность процедур контроля и обзора в достижении желаемых результатов. Показателем зрелости управления данными является организационное понимание и принятие остаточного риска, который определяет приоритетность действий. Организация, которая считает, что риска нарушения целостности данных нет, вряд ли сделала адекватную оценку рисков, присущих жизненному циклу данных. Поэтому следует подробно изучить подход к оценке жизненного цикла данных, их критичности и степень риска. Это может указывать на возможные виды сбоев, которые могут быть исследованы в ходе проверки.

Показатели качества для обеспечения целостности данных

63. Следует приводить регулярные обзоры показателей качества со стороны руководства, в том числе касающиеся целостности данных, с тем чтобы выявлять, передавать на вышестоящий уровень и своевременно решать важные вопросы. Следует проявлять осторожность и выбирать ключевые показатели эффективности таким образом, чтобы не занизить важность и приоритетность целостности данных.

64. Показатели качества охватывают следующие виды действий:

превентивные, ориентированные на надзор за правилами предотвращения нарушений целостности (например, уровень осведомленности операторов и (или) руководителей смен о целостности данных, полное время обработки образцов);

корректирующие, ориентированные на мониторинг соответствия выполнения и результатов записей в сравнении с критериями ALCOA+ (например, показатель оценки электронных записей, показатель корректирующих действий в отношение целостности данных);

мониторинг, ориентированный на контроль количества фактических нарушений целостности и соответствующих последующих действий (например, показатель внутренней проверки целостности данных, показатель самопроизвольных сбоев целостности, в том числе, сообщаемых операторами).

Для периодической проверки эффективности и контрольных мер в отношение указанных показателей, направленных на демонстрацию приверженности руководства обеспечению целостности управления данными в сфере GMP, целесообразно привлекать независимого эксперта

V. Требования к регулируемым бумажным записям

1. Система менеджмента качества для управления бумажными записями

65. Эффективное управление бумажными записями является ключевым элементом фармацевтической системы качества на любом этапе жизненного цикла продукции. Соответственно, система документации должна соответствовать положениям Правилам

производственной практики и обеспечивать эффективный контроль за документами и записями для поддержания их целостности.

66. Во всех случаях, когда бумажные записи создаются и используются для обеспечения безопасности пациентов и качества продукции, эти записи должны контролироваться и оставаться надежными на протяжении всего жизненного цикла данных, то есть соответствовать критериям ALCOA+.

67. Процедуры, описывающие надлежащую практику документирования и механизмы контроля документации, должны быть доступны в рамках системы менеджмента качества (СМК). Эти процедуры включают в себя:

создание, согласование и утверждение базовых документов (master documents) и процедуры для использования в течение их жизненного цикла;

создание, распространение и контроль шаблонов, используемых для записи данных (образцы, журналы и т. д.);

процессы извлечения и аварийного восстановления данных;

процесс создания рабочих копий документов (например, стандартных операционных процедур и бланков) для повседневного использования с особым акцентом на обеспечение контролируемости и прослеживаемости копий;

руководство по заполнению документов в бумажном виде с указанием способов идентификации отдельных сотрудников, форматов ввода данных и внесения изменений в документы;

порядок рутинной проверки заполненных документов на точность, подлинность и полноту;

процессы регистрации, поиска, хранения, архивирования и удаления бумажных записей.

2. Создание, распределение и завершение бумажных записей

Создание записей

68. Бумажные записи создаются в соответствии со следующим порядком:

всем документам присваивается уникальный идентификационный номер (включая номер версии). Все документы и проверяются, утверждаются, подписываются и датируются;

использование неконтролируемых документов и временных записей (например, на фрагментах бумаги) следует запретить внутренними процедурами;

форма документа должна обеспечивать достаточное пространство для внесения данных, с тем, чтобы обеспечить четкость и разборчивость записанных данных. Должно быть четко указано, какие данные должны быть вписаны в каждое предусмотренное для этого поле;

документы должны храниться таким образом, чтобы обеспечить надлежащий контроль версий;

неавторизованные или непреднамеренные изменения в основной копии (например, форма для заполнения, отдельно прикрепленная к стандартным операционным процедурам) не допускаются. Риск ненадлежащего использования и (или) фальсификации записи «обычными средствами» (то есть средствами не требующими использования специальных навыков мошенничества) следует снизить до приемлемого уровня.

69. Для типовых записей, хранящихся в электронном виде, принимаются следующие меры предосторожности:

осуществление контроля доступа к эталонным шаблонам;

управление процессами для создания и обновления версий должно быть четким, практичным и проверенным;

основные документы должны храниться таким образом, чтобы предотвратить несанкционированные изменения.

70. Мастер-копии должны содержать отличительную маркировку, позволяющую отличить мастер от копии (например, использование цветных бумаг или чернил для предотвращения случайного использования).

71. Перечень всех шаблонов записей управляется службой качества. В перечень для каждого типа записи следует включать как минимум, следующую информацию:

наименование, номер, включая номер версии записи;

местонахождение записи (например, база данных документации, дата вступления в силу, дата пересмотра и т. д.).

72. Записи в производственных зонах надлежащим образом контролируются назначенными лицами или определенными процессами. Эти меры контроля следует осуществлять таким образом, чтобы свести к минимуму риск повреждения или потери записей и обеспечить целостность данных

Распределение бумажных записей

73. Бумажные записи должны распределяться в соответствии со следующими правилами:

обновленные версии следует распространять своевременно, при этом только текущая утвержденная версия может быть доступна для использования;

устаревшие основные документы и файлы архивируются, а доступ к ним ограничивается;

все выданные и неиспользованные бумажные документы собираются и уничтожаются соответствующим образом;

выдача контролируется с помощью защищенного штампа или бумажного цветового кода, который не должен находиться в рабочих зонах или другой соответствующей системе;

незаполненные («пустые») документы следует идентифицировать с помощью уникального идентификатора, создание каждого документа нумеруется и записывается.

Ведение и завершение бумажной записи

74. Рукописные записи ведутся и завершаются в следующем порядке:

записи делаются лицом, выполнившим задание;

неиспользованные, пустые поля в документах перечеркиваются, датируются и подписываются;

записи выполняются четким и разборчивым почерком;

заполнение полей дат производится в формате, определенном для производственной площадки (например, ДД.ММ.ГГГГ);

внесение (выполнение) записей должно осуществляться своевременно;

записи должны быть нестираемыми. Использование карандашей, пишущих устройств с исчезающими (термочувствительными) чернилами не допускается;

записи подписываются и датируютсяс использованием уникального идентификатора, присваиваемого автору записи.

75. Следует обеспечить прослеживаемость любых определяемых пользователем параметров в рамках деятельности по обработке данных. Записи должны позволять восстанавливать всю деятельность по

обработке данных, независимо от того, сообщается ли о результатах этой обработки впоследствии или они используется иным образом. Если обработка данных повторяется с постепенным изменением параметров обработки, то это должно быть видимым для обеспечения того, чтобы параметры обработки не были использованы для достижения более желательной конечной точки.

76. Поправки в записях следует вносить таким образом, чтобы обеспечить полную прослеживаемость, в том числе применяя:

зачеркивание записи, которая подлежит изменению, способом, позволяющим прочитать зачеркнутое (например, одной линией);

указание причины исправления (где возможно), с ее фиксацией и проверкой, если это критично;

указание инициалов (Ф. И. О.) лица, внесшего изменения и даты их внесения.

3. Проверка записей

77. Подход к проверке содержания конкретных бумажных записей, таких как критические бумажные записи и соответствующие исправления, следует ориентировать на обеспечение проверки соблюдения критериев ALCOA+ и требований актов органов Союза в сфере обращения лекарственных средств.

78. У регулируемой компании должна существовать процедура, описывающая процесс проверки и утверждения данных. Проверку данных следует задокументировать протоколом. В протокол включается заключение о том, были ли обнаружены проблемы, дата проверки и подпись рецензента.

79. Процедура проверки должна содержать описание действий, которые следует предпринять, в случае если анализ данных выявит

ошибку или упущение и позволять корректировать или уточнять данные, чтобы обеспечить читаемость исходной записи и прослеживаемость ее коррекции с использованием критериев ALCOA+.

80. При наличии аутсорсинговых процессов фармацевтической компании следует гарантировать, что критические данные, полученные от поставщика, будут соответствующим образом рассмотрены и проанализированы с точки зрения их целостности. Ответственность за анализ данных следует документировать и согласовать обеими сторонами.

4. Истинные копии

81. Процесс создания истинной копии (печатной или электронной) следует атестовать и полностью описать, а копию заверить путем нанесения даты и подписи на бумагу или путем использования подтвержденной электронной подписи. Истинная копия может храниться в другом электронном формате по сравнению с первоначальной записью, если это необходимо, но должна сохранять эквивалентный статический и (или) динамический характер исходной записи.

Истинные копии бумажных документов

82. Истинные копии оригиналов бумажных записей (например, аналитические протоколы, валидационные отчеты и т. д.) полезны для целей коммуникации (например, между компаниями, работающими в разных местах). Эти записи следует контролировать в течение их жизненного цикла, чтобы гарантировать, что данные, полученные с другой площадки (дочерней компании, подрядчика и т. д.) сохраняются как истинные копии, когда это целесообразно, или используются в

качестве краткого отчета, когда требования, предъявляемые к истинной копии, не соблюдаются (например, резюме сложных аналитических данных).

83. Истинная копия должна обеспечивать сохранение полного смысла данных и возможность восстановления их истории.

84. Оригинальные записи и истинные копии должны сохранять целостность записи. Истинные копии оригиналов записей могут храниться вместо оригиналов записей (например, при сканировании бумажных записей), если существует документированная система проверки и записи целостности копии. Организации следует учитывать любой риск, связанный с уничтожением оригинальных записей.

Бумажные записи, полученные из компьютерных систем

85. Бумажные записи, генерируемые простыми электронными системами (например, такими как весы, pH-метры или простое технологическое оборудование), которые не хранят данные, предоставляют ограниченную возможность изменения представления указанных данных путем их обработки (в том числе повторной), изменения электронных меток даты (времени). В этих обстоятельствах оригинал записи подписывается и датируется лицом, создающим запись, а также включается в досье на серию.

86. Такой подход разрешен только для простых систем и для записей, содержимое которых статично.

87. Статический формат записи, такой как бумажная или электронная запись, является фиксированным и практически не допускает взаимодействия между пользователем и содержимым записи. Например, после печати или преобразования в статический

электронный формат записи теряют возможность повторной обработки или более детального просмотра исходных значений.

88. И наоборот, записи в динамическом формате, такие как электронные записи, допускают интерактивную связь между пользователем и содержимым записи. Например, электронные записи в форматах баз данных позволяют пользователю отслеживать тренды и запрашивать данные; записи хроматограмм, сохраняемые в электронном формате позволяют пользователю или проверяющему (при наличии соответствующих прав доступа) произвести повторную обработку данных и увеличить масштаб, чтобы просмотреть детали более четко.

89. Многие электронные записи важно сохранять в их динамическом (электронном) формате, чтобы обеспечить взаимодействие с данными. Выбор формата сохранения следует проводить с учетом возможных рисков, связанных с необеспечением целостности данных. Для такого рода записей не допускается ведение исключительно бумажных записей и удаление соответствующих электронных записей.

5. Хранение записей

90. Срок хранения каждого типа записей должен (как минимум) соответствовать срокам, указанным в соответствующих требованиях Правил надлежащей производственной практики, а также учитывать требования иных актов органов Союза в сфере обращения лекарственных средств, которые могут предусматривать более длительные сроки хранения. Записи могут храниться внутри организации или их хранение организуется с помощью внешней службы хранения, при условии подписания соответствующего соглашения.

91. Мероприятия по архивации следует организовать таким образом, чтобы обеспечивать возможность восстановления и читаемости данных и метаданных на протяжении всего периода их хранения.

6. Утилизация записей

92. Следует организовать документированный процесс удаления записей таким образом, чтобы обеспечить удаление данных, подлежащих удалению по истечении установленного срока хранения. Система должна гарантировать, что текущие записи не подвергнутся случайному уничтожению, и исторические записи непреднамеренно не будут возвращены в число текущих записей (например, исторические записи перепутаны и (или) перемешаны с существующими записями).

93. У регулируемой компании должна вестись запись (реестр) фиксирующая надлежащее и своевременное уничтожение изъятых из обращения записей.

94. Следует принять меры для снижения риска удаления непредусмотренных для уничтожения записей. Права доступа, позволяющие удалять записи, следует ограничить и предоставлять только ограниченному кругу лиц (как правило, несколько человек).

95. При использовании распечаток, которые не являются устойчивыми к хранению (перманентными) (например, термотрансферная бумага), заверенную («истинную») копию следует сохранить, а оригинал, не являющийся перманентным, допускается уничтожить. Бумажные документы могут быть заменены сканированными копиями при условии соблюдения принципов истинной копии, приведенных в пунктах 85 – 89 настоящего Руководства.

VI. Требования к регулируемым электронным записям

96. Регулируемые электронные записи (то есть создаваемые и используемые для обеспечения безопасности пациентов и качества продукции) управляются с помощью большого количества компьютерных систем, используемых компаниями в операционной деятельности. Эти системы варьируются от простых автономных до больших интегрированных и сложных систем, многие из которых влияют на качество продукции. Каждая регулируемая организация несет ответственность за полную оценку и контроль всех компьютеризированных систем и управление ими в соответствии с требованиями Правил надлежащей производственной практики.

97. Регулируемые компании должны быть в полной мере осведомлены о характере и областях задействования компьютеризированных систем и проводить оценку каждой системы, в том числе ее использования по назначению и функционирования, а также любые риски или уязвимости для целостности данных, которые могут быть подвергнуты воздействию. Особое внимание следует уделить определению критичности компьютеризированных систем и любых связанных с ними данных в отношении качества продукции.

98. Все компьютеризированные системы, потенциально влияющие на качество продукции, должны эффективно управляться в соответствии со «зрелой» системой качества, которая обеспечивает защиту систем от актов случайного или преднамеренного вмешательства, изменения или любых других действий, которые могут повлиять на целостность данных.

99. При определении уязвимостей и рисков для данных важно, чтобы компьютеризированная система рассматривалась в контексте ее использования в рамках бизнес-процесса.

100. Для обеспечения соответствия регулируемых электронных записей критериям ALCOA+, соответствующие компьютеризированные системы следует обеспечить надежность, безопасность, прослеживаемость, проверяемость и подотчетность.

101. Эти требования отражены в приложении 11 к Правилам производственной практики, в котором определяются нормативные требования к критическим записям, управляемым с помощью компьютеризированных систем, которые ориентированы на обеспечение целостности этих данных.

1. Валидация компьютеризированных систем

102. Компьютеризированные системы должны соответствовать требованиям актов органов Союза в сфере обращения лекарственных средств и применимым руководствам государств-членов, которые включают требования к валидации. Компьютеризированные системы должны быть валидированы для использования по назначению, что требует в процессе валидации понимания функций компьютеризированной системы в рамках конкретного бизнес-процесса.

103. Валидация компьютеризированной системы это документированный процесс достижения и поддержания ее соответствия применимым Правилам производственной практики и пригодности для целевого использования путем реализации принципов, подходов и мероприятий жизненного цикла в рамках валидационных планов и отчетов, а также путем применения соответствующих оперативных средств контроля на протяжении всего срока службы системы.

104. Для обеспечения целостности электронных данных компьютеризированные системы должны быть валидированы на уровне, соответствующем их использованию и применению. Валидация предусматривает необходимые меры контроля для обеспечения целостности данных, включая оригинальные электронные данные и любые распечатки или отчеты в формате PDF, полученные из системы. В частности, этот подход должен обеспечить выполнение критериев ALCOA+ и надлежащее управление рисками для целостности данных на протяжении всего жизненного цикла данных. При валидации компьютеризированных систем и при последующем контроле изменений следует внедрить все необходимые средства контроля для обеспечения целостности данных и (или) подтвердить, что они имеются в наличии, и, что возникновение ошибок в данных сведено к минимуму.

105. Мероприятия по валидации должны гарантировать, что параметры конфигурации и элементы управления для обеспечения целостности данных задействованы и управляются в вычислительной среде (включая программное обеспечение приложений и операционных систем). Указанные мероприятия включают в себя, но не ограничиваются следующим:

а) документирование спецификаций конфигурации для коммерческих «готовых» систем, а также разработанных пользователем систем, где применимо;

б) ограничение параметров конфигурации безопасности «администраторов системы» для независимого персонала, где это технически возможно;

в) отключение параметров конфигурации, позволяющих перезаписывать и повторно обрабатывать данные без возможности отслеживания;

г) ограничение применения штампов времени и (или) даты и (или) доступа к такой возможности применения.

106. Использование валидационных данных от поставщика системы в отрыве от ее конкретных конфигурации и назначения неприемлемо. В данном случае валидационные мероприятия поставщика следует рассматривать как своего рода функциональную верификацию, которая может не соответствовать требованиям к квалификации эксплуатации.

107. Настоящее руководство предлагает вариант интегрирования риск-ориентированного подхода к валидации компьютеризированных систем в бизнес-процессы, определяет документацию, требуемую для каждого из этапов валидации при таком подходе, и описывает ответственных участников на каждом шаге процесса валидации. В разделе VIII настоящего Руководства обобщен современный отраслевой опыт в области валидации компьютеризированных систем, основанных на оценке рисков, включая руководящие указания и методологию из руководящих принципов, соответствующих критериям PIC/S и ISPE.

Сбор (ввод) данных

108. Системы разрабатываются для правильного сбора (ввода) данных, полученных с помощью ручных или автоматизированных средств.

109. В системах для ручного ввода данных:

а) ввод данных осуществляется только авторизованными лицами, система должна регистрировать данные о входе, о лице, создающим запись, и времени и дате когда запись была сделана;

б) данные вводятся в предусмотренном формате, который контролируется программным обеспечением;

в) мероприятия по валидации должны подтвердить что недействительные форматы данных не принимаются системой сбора (ввода) данных;

г) все данные, введенные вручную, проверяются вторым оператором, либо валидированными компьютерными системами в том случае, если эти данные могут повлиять на качество продукции или безопасность пациента;

д) изменения в записях (включая причину внесения изменений) регистрируются в виде «контрольного следа» и проверяются соответствующим авторизованным и независимым лицом в соответствии с рисками для качества продукции и безопасности пациента.

110. В системах для автоматизированного сбора данных:

а) следует провести валидацию интерфейса между исходной системой, системами сбора и регистрации данных для обеспечения точности данных;

б) данные, полученные системой, сохраняются в памяти в формате, который не подвержен манипуляциям, потерям или изменениям;

в) программное обеспечение системы должно включать в себя валидированные проверки для обеспечения полноты полученных данных, а также любых метаданных, связанных с полученными данными;

г) все необходимые изменения данных должны одобряться (разрешаться) и контролироваться в соответствии с утвержденными в регулируемой компании процедурами. Например, ручная интеграция и повторная обработка результатов лабораторных исследований должны выполняться утвержденным и контролируемым образом. Службе

качества фармацевтической компании следует принять меры, обеспечивающие возможность внесения изменений в данные только в случае необходимости и только назначенными лицами.

2. Безопасность

Доступ к системе

111. Средства контроля доступа пользователей, как физические, так и электронные, должны быть сконфигурированы и применены для запрещения несанкционированного доступа, изменения и удаления данных.

112. Для всех сотрудников, нуждающихся в доступе и использовании конкретной электронной системы, устанавливаются и присваиваются индивидуальные логины и пароли. Общие учетные данные для входа не позволяют проследить за лицом, которое выполнил действие; по этой причине общие пароли (даже если они оправданы по причинам финансовой экономии) должны быть запрещены.

113. В случае если система не включает в себя функции контроля доступа (например, если для нее не требуется пароль, или если должна использоваться общая учетная запись пользователя), следует принять одну из следующих альтернативных мер контроля (эквивалентных между собой):

ведение журнала в бумажной форме, заполняемого вручную, обеспечивающего прослеживаемость обращений к системе;

установка в систему стороннего программного обеспечения, позволяющего обеспечить доступ к системе только предварительно авторизованным операторам.

Пригодность этих альтернативных мер контроля следует обосновать и задокументировать.

Авторизация пользователя

114. Следует в полной мере использовать механизмы контроля доступа для обеспечения того, чтобы сотрудники имели доступ только к функциям, соответствующим их служебной роли, и чтобы действия относились к конкретным лицам. Компании должны быть в состоянии продемонстрировать уровни доступа, предоставленные отдельным сотрудникам, и обеспечить наличие ретроспективной информации об уровне доступа пользователей.

115. Контроль доступа должен применяться как при входе в операционную систему, так и запуске (работе) приложений. Индивидуальный вход в систему на уровне операционной системы может не потребоваться, если имеются соответствующие средства управления для обеспечения целостности данных (например, невозможно изменить, удалить или создать данные вне приложения).

116. Доступ администратора к компьютерным системам, используемым для запуска приложений, должен контролироваться. Обычные пользователи не должны иметь доступа к критически важным аспектам программного обеспечения, например, к системному времени, функциям удаления файлов и т. д. Права системного администратора (разрешающие такие действия, как удаление данных, изменение базы данных или изменение конфигурации системы) не назначаются лицам, непосредственно заинтересованным в сохранении целостности данных (создание данных, просмотр или утверждение данных).

117. Схема авторизации пользователей должна обеспечивать разделение обязанностей.

Резервное копирование

118. Процессы резервного копирования и восстановления следует документировать с помощью процедуры, определяющей операции резервного копирования и шаги восстановления, которые выполняются в случае необходимости. Процессы резервного копирования и восстановления следует протестировать для обеспечения возможности полного восстановления данных и метаданных в случае сбоя системы. Следует создать механизм (автоматический или ручной) проверки резервного копирования для обеспечения его надлежащего функционирования.

119. Процессы резервного копирования и восстановления должны быть документированы (например, с помощью процедуры), валидированы и должны проходить периодическую проверку. Каждая резервная копия должна проверяться для обеспечения ее правильного функционирования.

120. Обычные резервные копии (например, носители, на которых хранятся копии данных) следует хранить в удаленном месте (физически раздельно) на случай возникновения аварийной ситуации.

Проверка переноса данных

121. Перенос данных – это процесс передачи данных и метаданных между типами носителей или компьютеризированными системами. При необходимости перенос данных может изменять формат данных, для того чтобы сделать их пригодными для использования или видимыми в альтернативной компьютерной системе.

122. Процедуры переноса данных должны содержать соответствующее обоснование и быть тщательно разработаны и

проверены для обеспечения целостности данных в течение жизненного цикла данных

3. Прослеживаемость

Контрольный след

123. Система должна обеспечивать автоматическую запись контрольного следа, который представляет собой форму метаданных, содержащих информацию, связанную с действиями, относящимися к созданию, изменению или удалению регулируемых электронных записей. Контрольный след обеспечивает безопасную запись сведений о жизненном цикле данных, таких как создание, добавление, удаление или изменение информации в записях, без искажения или перезаписи исходной записи. Контрольный след облегчает восстановление истории указанных событий, связанных с записью, независимо от ее носителя, включая информацию «кто, что, когда и почему», относящуюся к событию.

124. Записи контрольного следа должны быть иметь понятную форму и содержать по крайней мере следующую информацию:

а) идентификатор лица, внесшего изменение в данные;

б) описание изменения;

в) время и дату изменения;

г) причину внесения изменения.

125. Функции контрольного следа должны быть постоянно включены, а доступ к ним заблокирован. Как и другие функциональные возможности, направленные на обеспечение целостности данных, контрольный след должен верифицироваться в ходе валидации системы.

126. Система должна базироваться на надлежащим образом контролируемом и (или) синхронизированном времени для регистрации событий в привязке к нему с целью обеспечения возможности реконструкции и прослеживаемости, включая информацию о часовом поясе, в котором эти данные используются при наличии нескольких удаленных площадок. Операторам не разрешается изменять референтное время и (или) часовой пояс.

127. В случае отсутствия в системах автоматического контрольного следа, для фиксации изменений GMP -критичных данных в качестве временной меры могут быть использованы бумажные записи, но только до тех пор, пока система с функционирующим контрольным следом не станет доступной.

Проверка контрольного следа

128. Данные контрольного следа, относящиеся к регулируемым электронным записям, подлежат аудиту со стороны авторизованного пользователя с целью проверки правильности выполнения операций и внесения каких-либо изменений (модификации, удаления или перезаписи) в исходную информацию в электронных записях. Все изменения должны быть должным образом санкционированы.

129. Проверка связанных с данными релевантных контрольных следов должна быть частью рутинной проверки данных в процессе их утверждения.

130. Периодичность, функции и обязанности по проверке контрольного следа должны основываться на оценке риска в соответствии с релевантностью для GMP данных, записанных в компьютеризированной системе. Например, в случае изменений в электронных данных, которые могут оказать непосредственное влияние

на качество лекарственных средств, ожидается, что контрольный след будет проверяться каждый раз, когда указанные данные генерируются или используются (то есть когда данные используются для принятия GMP-критического решения).

131. Регулируемый пользователь должен разработать документированную процедуру, которая подробно описывает, как следует проверять контрольный след. Процедура должна подробно определять процесс, которому должно следовать лицо, ответственное за проверку контрольного следа.

132. Действия, связанные с контрольным следом, должны быть документированы. С указанными записями следует обращаться так же, как и с другими документами, подпадающими под действие GMP.

4. Проверяемость

Электронные копии

133. Система должна позволять создавать точные и полные копии записей как в читаемой, так и в электронной форме, пригодные для проверки, оценки и копирования со стороны проверяющих лиц.

Архивирование данные

134. Данные должны периодически архивироваться в соответствии с письменными процедурами. Архивные копии и резервные копии данных должны физически сохраняться в разных местах.

135. Данные должны быть доступными и читаемыми, а их целостность должна поддерживаться на протяжении всего периода архивирования.

136. Должна быть предусмотрена процедура восстановления архивных данных в случае необходимости проведения расследования. Процедура восстановления архивных данных должна регулярно проверяться.

137. В случае прекращения поддержки устаревших систем, следует рассмотреть вопрос о поддержании программного обеспечения в состоянии, обеспечивающем доступ к данным (как можно дольше, в зависимости от конкретных требований к хранению). Это может быть достигнуто путем поддержки программного обеспечения в виртуальной среде.

138. С увеличением возраста устаревающих данных может потребоваться их миграция в альтернативный формат файла, который сохраняет как можно больше атрибутов «истинной копии» данных. В случаях, когда миграция исходных данных с полной функциональностью технически невозможна, следует оценить возможные варианты, учитывая риски и важность данных с течением времени. Формат файла миграции должен быть выбран с учетом баланса риска между долгосрочной доступностью и возможностью снижения функциональности динамических данных.

Удаление данных

139. Должны быть разработаны процедуры, описывающие процесс удаления хранящихся в электронной форме данных. Эти процедуры должны содержать руководство для оценки данных и их нахождения в период хранения, а также описывать порядок удаления данных, которые более не требуются.

5. Контроль и учет

Электронная подпись

140. Электронные подписи, используемые взамен рукописных подписей, должны контролироваться для подтверждения их аутентичности и прослеживаемости относительно конкретного лица, подписавшему запись.

141. Использование электронной подписи должно контролироваться, при этом особый контроль применяется к следующим процессам:

закреплению подписи за ее владельцем;

регистрации факта электронной подписи в системе, таким образом, чтобы его нельзя было подделать или изменить без аннулирования подписи или статуса записи;

связи внесенной подписи с выполненной записью, и возможности проверки этого процесса;

защите электронной подписи, таким образом чтобы она могла применяться только «владельцем» этой подписи.

142. Для подтверждения пригодности и контроля в отношение подписанных записей следует проводить надлежащую валидацию связанного с системой процесса подписи.

143. В случае подготовки бумажной или PDF-копии документа с электронной подписью, метаданные, связанные с электронной подписью, должны сохраняться вместе с соответствующим документом.

144. Электронная подпись или системы электронной подписи должны предусматривать «проявления подписи», то есть отображение в пределах видимой записи того, кто поставил подпись, должность

подписавшего (где возможно), дату (и время, если это значимо), а также значение подписи (например, «проверено» или «утверждено»).

145. Вставленное изображение подписи или сноска, указывающая на то, что документ был подписан в электронной форме (если он был введен способом, отличным от валидированного процесса электронной подписи), являются недостаточными. Если документ подписан в электронной форме, то метаданные, связанные с подписью, сохраняются.

VII. Риск – ориентированный подход к жизненному циклу валидации

146. Компьютеризированные системы, которые могут влиять на качество продукции или услуг и целостность данных, подпадают под действие правил GMP и нуждаются в валидации.

147. В настоящем разделе описан подход к процессу валидации компьютеризированной системы на протяжении всего жизненного цикла системы в соответствии с принципами PIC/S и GAMP, а также определены процедурные рамки, обеспечивающие выполнение требований Правил производственной практики в результате процесса валидации. Настоящий раздел определяет действия, которые должны быть выполнены до выпуска компьютеризированной системы в эксплуатацию, во время ее использования вплоть до момента вывода компьютеризированной системы из эксплуатации.

148. Процесс валидации обеспечивает документированное доказательство, позволяющее с высокой степенью уверенности сделать вывод о том, что компьютеризированная система функционирует в соответствии с ее спецификациями, а также требованиями к качеству и нормативным требованиям на постоянной и воспроизводимой основе.

Кроме того, процесс валидации должен обеспечить документальное подтверждение того, что система включает в себя автоматизированные функции, ориентированные на обеспечение соответствия требованиям GMP для критических электронных записей критериям ALCOA+.

149. Настоящее Руководство использует риск-ориентированный подход к разработке спецификации, проектированию и проверке компьютеризированных систем, которые могут повлиять на качество продукции и безопасность пациентов на следующих этапах:

а) определения требований и планирования, поскольку этот этап ориентирован на постановку необходимых задач, распределение обязанностей, определение процедур и сроков с учетом рисков, связанных с системой;

б) подготовки проекта внедрения, который основан на документированной спецификации требований пользователей (URS), ориентированной на детализацию потребностей бизнеса и пользователей (с точки зрения бизнес-процессов, соответствия требованиям, а также технических и нефункциональных стандартов), которые будут определены на начальных этапах проекта внедрения;

в) спецификации и создания компьютеризированной системы, на котором на основе спецификации требований пользователей поставщик (исполнитель) создает набор документированных спецификаций для определения конструкции (конфигурации) системы. Количество и уровень детализации спецификаций при этом могут варьироваться в зависимости от типа системы и ее предполагаемого использования. На этапе квалификации проекта создается матрица прослеживаемости, демонстрирующая взаимосвязь между спецификациями, соответствующими требованиями, и выполнением проверки исходного кода в случае системы, разработанной на заказ;

г) тестирования и приемки компьютеризированной системы, во время которых проверка системы направлена на подтверждение того, что спецификации были выполнены: это может включать несколько этапов проверки и тестирования в зависимости от типа системы, применяемого метода разработки и его использования. Тестирование должно основываться на результатах оценки функциональных рисков;

д) выпуска компьютеризированной системы в эксплуатацию, при котором система официально принята к использованию и инсталлирована в операционную (производственную) среду в соответствии с контролируемым и документированным процессом, включая утверждение от владельца бизнес-процесса, технического владельца и представителей службы качества;

е) работы компьютеризированной системы через вспомогательные процессы, при которой после выпуска в эксплуатацию система управляется через вспомогательные процессы, ориентированные на поддержание ее валидированного статуса;

ж) завершения эксплуатации компьютеризированной системы, при которой система выводится из эксплуатации, но данные, поддерживаемые системой, должны быть доступны в течение срока их хранения.

150. Оптимальным вариантом является проведение перспективной валидации компьютеризированных систем; однако для уже установленных систем может быть приемлемым проведение ретроспективной валидации на основе оценки всех исторических данных (данные которые уже были произведены системой).

1. Компьютеризированные системы и категоризация

151. Риск сбоев или дефектов как правило, повышается с повышением доли пользовательского программного и аппаратного обеспечения по сравнению с долей стандартного программного и аппаратного обеспечения. Повышенный риск обусловлен сочетанием большей сложности и меньшего опыта пользователей. Категоризация в сочетании с оценкой рисков и оценкой поставщиков может быть частью эффективного подхода к управлению рисками для качества.

152. Компьютеризованная система считается состоящей из всего аппаратного обеспечения, прошивки (микропрограммного обеспечения), установленных устройств и программного обеспечения, контролирующего работу компьютера (как это показано на рисунке). Контролируемая функция может состоять из оборудования, подлежащего контролю, и оперативных процедур, контролирующих это оборудование, или же это может быть операция, для которой не требуется оборудование, отличное от имеющегося аппаратного обеспечения.

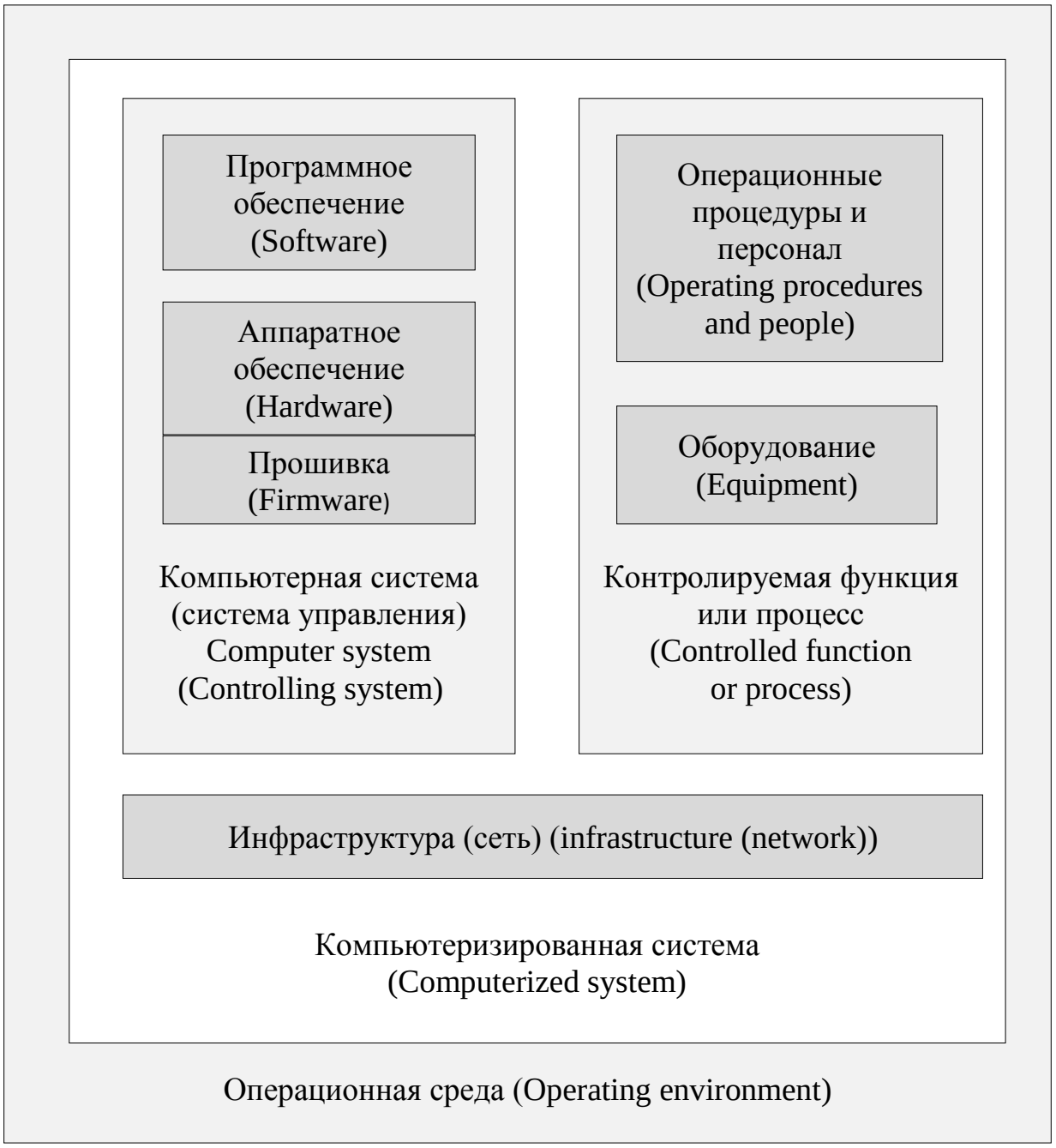

Рисунок. Схема взаимосвязи различных компонентов компьютеризированной системы в ее операционной среде

153. В большинстве систем имеются компоненты различной сложности, такие как операционная система, несконфигурированные компоненты и настроенные или настраиваемые компоненты. Для оптимизации выбора стратегии проверки и глубины ее проведения следует классифицировать системы по категориям, согласно таблице.

Таблица

Категории компьютеризированных систем

Категория	Тип	Описание	Примеры
1	Инфраструктурное программное обеспечение	Элементы инфраструктуры соединяются вместе, образуя интегрированную среду для запуска и поддержки приложений и сервисов	Установленное или коммерчески доступное многоуровневое программное обеспечение (операционные системы, менеджеры баз данных, языки программирования, промежуточное программное обеспечение, интерпретаторы релейной логики, инструменты статистического программирования и пакеты электронных таблиц (за исключением приложений, разработанных с использованием этих пакетов) Инструменты программного обеспечения инфраструктуры (например, программное обеспечение для мониторинга сети, инструменты планирования пакетных заданий, программное обеспечение для обеспечения безопасности, антивирусные программы и инструменты управления конфигурацией)
3	Неконфигурированные компоненты	Параметры времени выполнения могут быть введены и сохранены, но программное обеспечение не может быть настроено в соответствии с бизнес-процессом	Прошивки-приложений Программное обеспечение готовое к использованию (COTS - Commercial Off-The-Shelf) Инструментарий

Категория	Тип	Описание	Примеры
4	Конфигурированные компоненты	Коммерческое программное обеспечение, в том числе сложное, которое может быть настроено пользователем для удовлетворения конкретных потребностей бизнес-процесса пользователя Программный код не изменяется	Лабораторная система управления информацией (LIMS) Системы сбора данных Диспетчерский контроль и сбор данных (SCADA) Планирование ресурсов предприятия (ERP) Мониторинг клинических испытаний Распределенная система управления (DCS) Отчетность о побочных реакциях на лекарства (ADR) Система данных хроматографии (CDS) Система электронного документооборота (СЭД) Система управления зданием (BMS) Управление взаимоотношениями с клиентами (CRM) Электронные таблицы Простой человеко-машинный интерфейс
5	Пользовательские приложения	Программное обеспечение самостоятельно разработанное и закодированное пользователем с учетом бизнес-процессов	Самостоятельно разработанные приложения или приложения разработанные на заказ Стандартные компьютерные приложения Приложения, управляющие процессом Пользовательские схемы логики Электронные таблицы (макросы)

154. Как правило, уровень детализации и глубина подтверждающей документации должны возрастать с увеличением категории системы.

155. Сложные компьютеризированные системы могут состоять из нескольких компонентов, которые могут относиться к различным категориям. В этом случае система должна быть классифицирована в соответствии с высшей категорией множественных компонентов.

156. В случае, если один или ограниченное количество компонентов разработаны на заказ, систему можно все еще отнести к категории 4, а список разработанных на заказ компонентов, классифицировать по категории 5.

2. Инвентаризация компьютеризированной системы и оценка GMP рисков

157. Регулируемые компании должны иметь перечень всех используемых компьютеризированных систем, включающий в себя следующие данные:

а) наименование и номер версии системы, наименование поставщика системы, наименование владельца системы, местоположение и основные функции системы (то есть предполагаемое использование) каждой компьютеризированной системы;

б) оценку рисков, связанных с системой и соответствующими записями, которые управляются этой системой (например, прямое воздействие на GMP, косвенное воздействие, не влияет);

в) текущий статус валидации каждой системы и ссылки на существующие валидационные документы.

158. Для каждой системы проводится оценка рисков, в частности оценка необходимых мер контроля для обеспечения целостности

данных. Уровень и глубина валидации системы для обеспечения целостности данных определяются на основе критичности системы, процесса и потенциального риска для качества продукции, например, процессы или системы, которые генерируют или контролируют данные о выпуске серии, как правило, требуют большего контроля, чем те системы, которые управляют менее важными данными или процессами.

159. Объем валидации должен включать критерии приемлемости с точки зрения требований GMP, ранжированные по критичности риска для качества продукции (процесса), целостности данных, риска отказа или сбоя системы. Этот процесс представляет собой одно из наиболее важных предварительных условий планирования валидации, поскольку необходимо определить приоритеты и обратить внимание на системы, которые могут оказать влияние на качество продукции, безопасность пациента и целостность данных. Результаты анализа рисков и обоснование критических или некритических классификаций должны быть задокументированы. Риски, потенциально влияющие на соответствие GMP, должны быть четко определены.

160. Автоматизированное оборудование может быть перечислено в отдельном списке, необходимо избегать дублирования позиций в списках автоматизированного и компьютеризированного оборудования.

3. Оценка поставщика и соглашение о качестве

161. Когда третьи лица (например, поставщики оборудования, поставщики услуг или собственный IT отдел) привлекаются для обеспечения, установки, настройки, интегрирации, валидации, проведения технического обслуживания (например, через удаленный доступ), модификации или архивации компьютеризированной системы или соответствующих сервисов по обработке данных, следует

заключить и подписать официальное соглашение о качестве между регулируемой компанией и привлекаемым третьими лицами, с четким определением обязательств каждой из сторон.

162. Потенциальные и существующие поставщики GMP-критичных систем (поставщики компьютеризированных систем и поставщики услуг) оцениваются на основе бизнес-риска и влияния рассматриваемой услуги или компьютеризированной системы.

163. Оценка систем качества третьей стороны (в качестве компонента оценки рисков) проводится в целях определения объема валидационных мероприятий, а также для оценки возможности использования документации третьей стороны в рамках этого процесса. Цель проведения оценки третьей стороной заключается в определении того, отвечают ли поставщики компьютеризированных систем и поставщики услуг следующим требованиям:

а) способности обеспечить высокое качество продукции или услуг;

б) соответствие требованиям, сформулированным заказчиком;

в) наличие адекватных процессов обеспечения качества.

164. Анализ поставщика системы следует выполнить с целью проверки возможности создавать продукт, соответствующий стандарту качества и методологии. Выбранный в соответствии с процедурой оценки поставщиков метод должен основываться на анализе рисков, связанных с системой, сложности системы и предыдущем опыте работы с данным поставщиком.

4. Указания по организации валидации компьютеризированной системы на этапе планирования

Спецификация требований пользователя

165. Для всех компьютеризированных систем следует разработать спецификации требований пользователя, которые определяют назначение и функции системы, включая все основные требования к ней.

166. Объем и детализация требований должны быть соизмеримы с риском, сложностью и новизной и должны быть достаточными для поддержки последующего анализа риска, спецификации, конфигурации (дизайна) и проверки по мере необходимости.

167. В спецификации требований пользователя указывается, хранятся ли данные, управляемые системой, в электронном формате и используются ли данные для операций, оказывающих влияние на GMP.

168. Спецификация требований пользователя включает в себя следующее:

а) критически важные для качества функции;

б) идентификацию регулируемых электронных записей (ЭЗ), поддерживаемых системой, и подписываемых электронной подписью (ЭП), выполняемой в системе;

в) применимые требования актов органов Союза и законодательства государств-членов к электронным записям и управлению электронными подписями («правила ЭЗЭП»);

г) список бизнес-процессов и связанных с ними потоков процессов;

д) другие общие требования (например, эксплуатационные требования, требования к данным, технические требования, требования

к интерфейсу, требования к среде, требования к производительности, требования к доступности и требования к безопасности), которые включаются в спецификации требований пользователей по мере необходимости в зависимости от типа и сложности системы.

169. Требования определяются и согласовываются владельцем (владельцами) бизнес-процесса и включаются в соответствующие соглашения с уникальной кодировкой.

170. Спецификация требований пользователя считается обязательной также в случае ретроспективной валидации для определения назначения системы, которую следует верифицировать посредством интеграционного (end-to-end) теста.

План валидации

171. План валидации – это стратегический документ, подтверждающий, что все валидационные мероприятия проводятся должным образом под контролем руководства с использованием риск-ориентированного подхода.

172. План валидации определяет жизненный цикл валидации и объем валидации путем определения границ системы. Результаты оценки поставщика следует рассматривать вместе с условиями использования документации, предоставленной поставщиком.

173. В плане валидации должны быть идентифицированы:

а) перечень создаваемой документации;

б) распределение ответственности (например, матрица распределения ответственности RACI (ответственный, подотчетный, консультированный, информированный)) для результатов валидации;

в) общие критерии приемлемости для валидационного процесса.

174. План валидации всегда создается в случае внедрения новой системы или значительных изменений существующей.

5. Спецификации на этапе создания компьютеризированной системы

175. В зависимости от категории и сложности компьютеризированной системы документация по спецификации может быть объединена в один документ.

Функциональная спецификация

176. Функциональные спецификации должны содержать точное и подробное описание того, каким образом система удовлетворяет основным требованиям, предъявляемым к компьютерной системе и внешним интерфейсам. Это включает в себя описания функций, представлений и, где применимо, ограничений и атрибутов. Документ определяет, что должна делать система, и какие функции и средства разрешены системой, включая перечень проектных целей системы.

177. Документ должен содержать подробные функциональные описания требований компании к системе, диаграммы использования, технологические схемы, спецификации процессов, спецификации внешних интерфейсов, рабочие спецификации, спецификации безопасности и контроля, конфигурируемые элементы, детали логической модели данных, спецификации технологической инфраструктуры, спецификации доступности (ремонтопригодности)к.

178. Спецификации следует подготовить и организовать таким образом, чтобы можно было отслеживать каждое требование пользовательской спецификации, соотнося их с соответствующими функциональными возможностями и соответствующей документацией

по испытаниям, что обеспечивает прослеживаемость на протяжении всего жизненного цикла от индивидуальных требований пользователя до соответствующих испытаний. Описания «верхнего» уровня следует разделить на «подуровни», описывающие отдельные функции. Каждая функция должна иметь систему кодирования, с тем чтобы ее можно было идентифицировать и отслеживать.

179. Функциональные спецификации следует проверить на соответствие требованиям пользователя, что позволяет выполнять квалификацию эксплуатации (OQ) (то есть функциональное тестирование) и утверждение проектных спецификаций системы.

Конфигурационные спецификации.

180. Конфигурационная спецификация создается для описания:

списка компонентов аппаратного и программного обеспечения, включенных в компьютеризированную систему;

параметров системы (например, длины пароля), которые могут повлиять на одну или несколько функций в системе GMP.

181. Конфигурационная спецификация определяет базовые показатели конфигурации системы, адресующиеся к компонентам и интерфейсам программного обеспечения, а также параметрам системы, преимущественно фокусируясь на элементах конфигурации, которые могут повлиять на GMP-функциональные возможности.

182. Для идентификации профилей пользователей, определенных в системе, и связанных с ними функций создается Матрица безопасности (включенная в конфигурационную спецификацию или как отдельный документ). Соотнесение пользователей каждому профилю выполняется в соответствии с процедурами безопасности.

183. Конфигурационная спецификация должна также описывать IT-ландшафт, на котором размещено программное обеспечение, и то, как оно должно быть подключено к любой существующей системе или оборудованию. Поэтому этот документ должен включать также (или давать ссылку на другой документ) описание системного ландшафта и спецификации всех элементов, показанных на ландшафте (например, операционной системы, промежуточного программного обеспечения, вспомогательные инструменты - например, программы просмотра PDF-файлов, системных сред, интерфейсов, соответствующих компонентов IT-инфраструктуры (например, серверов)).

Проектные спецификации

184. Проектные спецификации необходимы для пользовательских компонентов в целях того, чтобы обеспечить детальное техническое описание функциональной спецификации, чтобы объяснить, как система выполняет то, что определено в спецификации высшего уровня.

185. Программное обеспечение должно быть разработано в соответствии с признанными стандартами проектирования, где это применимо. Проектные спецификации, определяя проект программного обеспечения, необходимы для разработанных на заказ приложений: этот тип документации как правило, не требуется для конфигурируемых продуктов, для которых проект программного обеспечения, как правило, рассматривается и оценивается в ходе оценки поставщика.

186. Проект программного обеспечения выполняется на двух уровнях. На более высоком уровне он определяет программные модули (подсистемы), которые формируют полную программную систему, интерфейсы между этими модулями, а также интерфейсы к другим внешним системам. На нижнем уровне проект описывает работу

отдельных программных модулей. Для кастомизированных компонентов проектная спецификация должна документировать компоненты разработки программного обеспечения, единицы реализации, дизайн пользовательского интерфейса, дизайн интерфейса, процедуры обработки ошибок и модели физических данных.

Детальная оценка рисков

187. Подробная оценка рисков требуется на этапах спецификации и создания системы посредством выполнения процессного и/или функционального анализа рисков с целью идентификации тех из них, которые могут повлиять на правильное или надежное функционирование системы на уровне процессов и функций соответственно.

188. Оценка функциональных рисков определяет соответствие нормативным требованиям и степень серьезности бизнес-рисков в сравнении с существующими функциональными возможностями системы и поддерживаемыми бизнес-процессами.

189. Валидационные группы вместе с владельцем бизнес-процесса или его представителями и техническими группами готовят оценку риска на основе требований пользователя и (или) функциональных, конфигурационных, проектных спецификаций.

190. Результат оценки риска должен включать результаты процессного и (или) функционального анализа риска, выполненного в соответствии с заранее определенной методологией

191. В отчете об оценке рисков должны быть определены действия по снижению риска, включая описание объема тестирования и ресурсов.

6. Фаза испытаний и приемки

192. Тестирование системы выполняется для проверки соответствия компьютеризированной системы требованиям, определенным до ее выпуска.

193. Объем работ по валидации на этапе тестирования и глубина документации по результатам зависит от таких масштабирующих факторов, как уровень GMP-риска системы и результат детальной оценки риска, которая выявила процессы и (или) функции с максимальными рисками, на которых должно быть сосредоточено тестирование.

194. Стратегия испытаний определяет соответствующий подход к испытанию конкретной системы, основанный на:

а) понимании компонентов системы (категория GAMP), общей сложности системы и новизны системы;

б) уровне GMP-риска системы;

в) результатах оценки функциональных рисков;

г) результатах оценки поставщиков, если это применимо.

195. Стратегия испытаний может варьироваться в широком диапазоне, например, от простого программного обеспечения с низким уровнем GMP-рисков до сложного программного обеспечения с высоким уровнем GMP-рисков. Стратегия испытаний определяется на как можно более ранних этапах жизненного цикла проекта, и предпочтительно параллельно с разработкой спецификаций системы.

196. Испытания системы следует организовать на разных фазах внедрения системы в процесс непрерывного мониторинга качества. Испытания системы включают в себя:

а) испытания от поставщика (например, тестирование ввода в эксплуатацию, модульное и интеграционное тестирование), выполняемое поставщиком ПО в соответствии с его системой качества или предопределенным планом качества и проекта;

б) валидационные испытания, выполняемые в квалификационной и (или) производственной среде по заранее определенным протоколам для следующих этапов:

в) квалификацию монтажа;

г) квалификацию функционирования;

д) квалификацию эксплуатации.

197. В случае если оценка поставщика определяет, что его методы управления качеством и практики проведения испытаний являются надлежащими, испытания, проведенные поставщиком в рамках жизненного цикла разработки программного обеспечения, могут быть использованы для сокращения усилий, предпринимаемых регулируемой компанией в отношение валидации, (применительно только для квалификации монтажа и функционирования). Валидационная документация, предоставляемая поставщиком, должна быть официально оценена, рассмотрена и одобрена регулируемой компанией.

Любой подключенный инструмент и (или) оборудование и соответствующие компоненты IT-инфраструктуры, включенные в компьютеризированную систему, проходят квалификацию до начала этапа IQ системы для демонстрации надлежащего функционирования и калибровки подключенных инструментов.

198. Документация по испытаниям (например, протокол квалификации) должна описывать подход к предполагаемому тестированию, среду тестирования, перечень испытаний и соответствующие критерии приемлемости, результаты испытаний

вместе с выявленными отклонениями (если таковые имеются) и критерии для различных этапов приемки. Этапы испытаний могут быть объединены (например, квалификация монтажа IQ и квалификация функционирования OQ) в случаях, когда это возможно. Результаты этапов испытаний должны быть документированы.

Системная среда

199. Испытания выполняются в квалифицированной соответствующим образом среде, по заранее разработанному плану испытаний с использованием разработанных спецификаций тестирования, включающих заранее определенные ожидаемые результаты.

200. Среды, используемые для разработки и (или) внедрения автоматизированной системы, могут различаться в зависимости от категории и сложности системы.

201. Создание среды разработки, квалификации (также называемой средой качества или средой валидации) и производственной среды рассматривается и документируется в конфигурационной спецификации и верифицируется (по крайней мере, для среды квалификации и производственной среды). Для документального подтверждения того, что среда квалификации эквивалентна производственной среде, должны быть выполнены соответствующие верификационные мероприятия.

Миграция данных

202. Миграция данных в значительной степени зависит от конкретной технологии и файловой структуры переносимых электронных записей.

203. Там, где это возможно, действия по миграции данных должны включать использование программных средств для автоматизации некоторых или всех операций их извлечения, преобразования, загрузки и проверки. Инструменты должны быть пригодны для использования по назначению. «Строгость» спецификации инструмента и действий по верификации должны быть соизмеримы с рисками.

204. При каждой миграции данных (либо внутри платформы системы, либо из одной системы в другую) и при преобразовании их состояния, данные должны быть проверены.

205. Эта проверка дает объективные доказательства того, что программные средства переноса данных подходят для использования по назначению, а также обеспечивает уровень уверенности в общем процессе переноса. Типичным подходом на этом этапе является работа с относительно небольшим объемом данных, который впоследствии может быть полностью проверен, чтобы гарантировать отсутствие ошибок данных.

Протокол квалификации монтажа

206. Квалификация монтажа (IQ) (также называемая конфигурационным тестированием) – это деятельность по проверке установки и конфигурации аппаратных и программных компонентов системы и соответствующей документации.

207. Квалификация монтажа должна осуществляться после «замораживания» конфигурации, которая подлежит проверке. Любые изменения, внесенные позднее в конфигурацию, должны пройти процедуру управления изменениями.

208. При квалификации монтажа надо учитывать условия, в которых будут проводиться испытания. Как правило, настоятельно рекомендуется специальная среда тестирования. В ходе IQ должны быть выполнены необходимые контрольные мероприятия, чтобы дать документальное подтверждение того, что испытательная и производственная среда эквивалентны.

209. Квалификация всех подключенных инструментов (оборудования) и соответствующей IT-инфраструктуры рассматривается в качестве предварительных условий для этапа квалификации монтажа.

210. Протокол квалификации монтажа определяет испытания, которые должны проводиться для компьютеризированной системы. Он должен содержать по крайней мере следующие этапы проверки:

а) правильность установки аппаратного и программного обеспечения в соответствии с техническими характеристиками и базовыми показателями конфигурации системы;

б) соответствие настройки конфигурации тому, что указано в конфигурационных спецификациях (если применимо);

в) наличие документации по системе.

211. Для разработки протокола квалификации монтажа стандартного программного обеспечения может быть использована документация поставщика: процедуры, руководства, инструкции.

Протокол квалификации функционирования

212. Цель квалификации функционирования (OQ) состоит в том, чтобы продемонстрировать, что система и каждая из ее функций (процессов), идентифицированных как критические, работает в соответствии со спецификацией.

213. Тестирование должно основываться на утвержденных спецификациях (функциональные спецификации, спецификации требований пользователя и т. д.), а также результатах детальной оценки рисков для определения типологии тестов. Тесты по наихудшему сценарию проводятся для критических функций, и особое внимание следует обратить на представление результатов тестирования, предельных значений параметров системы, предельных значений данных и обработки ошибок.

214. Если система управляет регулируемыми электронными записями и подписями, протокол квалификации функционирования должен содержать также тесты, направленные на обеспечение мер контроля для обеспечения целостности данных (в соответствии с пунктами 102 – 110 настоящего Руководства). Кроме того, если тестирование соответствия общим нормативным требованиям включено в функции документированного контроля, реализуемые поставщиком, то на этапе квалификации функционирования регулируемая компания должна проводить верификацию этих функций, отвечающих за соответствие нормативным требованиям (например, контрольные следы, защита), применительно к конкретной среде и предполагаемому использованию.

215. Каждое испытание проводится с использованием заранее определенных данных и сценариев. Полученные результаты сопоставляются с ожидаемыми, получаемыми из функциональных спецификаций.

216. В случае использования для целей валидации автоматизированных средств тестирования, они должны быть оценены на предмет их адекватности.

Протокол квалификации эксплуатации

217. Этап квалификации эксплуатации (PQ) (также называемый верификацией требований) ориентирован на демонстрацию того, что система работает эффективно и воспроизводимо, пригодна для использования по назначению, и что система и ее операционная среда (включая пользователей) готовы к запуску в производство.

218. Квалификация эксплуатации PQ должна выполняться, в основном, назначенными представителями пользователей и должна быть ориентирована на подтверждение того, что:

а) этапы IQ-OQ завершены, и соответствующие отчеты утверждены, а любое отклонение проанализировано и «закрыто»;

б) все связанные с системой стандартных операционных процедур (СОП), руководства по установке и администрированию и руководства пользователя утверждены и доступны;

в) все пользователи, которые могут получить доступ к системе, обучены, а записи подтверждающие обучение доступны;

г) доступ для каждого пользователя был создан в соответствии с его навыками и обязанностями;

д) проверка бизнес-процессов, поддерживаемых системой («сквозные» тесты), основана на результатах детальной оценки рисков;

е) выполнимо восстановление системы и данных в рабочей среде (резервное копирование и восстановление данных).

219. Тесты PQ осуществляется в квалификационной среде. В случае, если такой подход невозможен по техническим причинам, PQ может быть выполнен непосредственно в производственной среде после повторения IQ в производственной среде.

Матрица прослеживаемости

220. Матрица прослеживаемости создается для подтверждения того, что:

а) бизнес-процессы были правильно переведены на системный функционал;

б) системный функционал и бизнес-процессы были должным образом испытаны в квалификационных тестах в соответствии с результатом детальной оценки риска.

7. Фаза ввода в эксплуатацию

221. Решение о начале использования компьютеризированной системы в производстве должно быть одобрено, по крайней мере, владельцем бизнес-процесса и службой качества. Эти роли определяют валидационный статус системы перед авторизацией развертывания в рабочей среде. Это решение должно быть официально задокументировано в разделе валидационного отчета или в специальном документе.

Валидационный отчет

222. В валидационном отчете собраны описания действий и соответствующих документов, с целью демонстрации правильного и полного выполнения процесса валидации в соответствии с планом. Валидационный отчет обеспечивает анализ данных, собранных в ходе процесса валидации, и документирует все результаты валидационной деятельности, включая любые несоответствия и последующие меры.

223. Валидационный отчет (краткий валидационный отчет) включает в себя:

а) четкое утверждение того, что система проверена и выпущена для рабочего использования;

б) идентификацию возможных ограничений;

в) подтверждение того, что все испытания были выполнены в соответствии с планом или утвержденным отклонением от плана;

г) измеримую оценку результатов испытаний и подтверждение соответствия критериям приемлемости системы;

д) план действий (если применимо);

е) обновленный список документации (основной список, включающий процедуры операционной среды, инструкции и элементы управления, которые регулируют использование и управление системой после ее выпуска.

224. После утверждения валидационного отчета реестр компьютеризированных систем должен быть обновлен, чтобы отразить подтвержденный статус системы и включить ссылку на валидационный отчет.

8. Вспомогательные процессы

Управление защитой

225. Для обеспечения высокого уровня защиты данных от потери конфиденциальности, потери целостности и предотвращения несанкционированного доступа с учетом системной среды, сетей и установленных программ, должны быть определены и внедрены процедуры безопасности.

226. Следующие процессы должны выполняться на протяжении всего жизненного цикла компьютеризированной системы:

а) физическая безопасность, которая включает в себя все соответствующие меры предосторожности для контроля доступа и среды для защиты объектов компьютеризированных систем от кражи, разрушения, неконтролируемого изменения или нарушения;

б) логическая безопасность, которая включает в себя все меры предосторожности для защиты программ и данных от несанкционированного доступа, неправильного использования или манипулирования, например, защита от вирусов, защита от внешних угроз, процедуры идентификации пользователей, контрольный журнал для созданных, измененных или удаленных данных;

в) ролевая безопасность должна быть внедрена для обеспечения доступа к GMP данным только предварительно авторизованным операторам в соответствии с соответствующей ролью в организации, сохраняя разделение обязанностей. Процедуры управления безопасностью применяются ко всем пользователям, включая администраторов, «суперпользователей», конечных пользователей и сотрудников службы поддержки (включая сотрудников службы поддержки от поставщиков).

227. Должны существовать контрольные процедуры для обеспечения:

а) установления и поддержки ролей и обязанностей в области защиты, политик, стандартов и процедур;

б) выполнения мониторинга защиты и периодического тестирования, например, ручную проверку журнала доступа к системе, автоматическое уведомление о блокировках, тестирование токенов (если таковые имеются);

в) создания и ведения списка лиц, имеющих право доступа к системе.

228. Конфигурация защиты документируется в спецификациях конфигурации системы или в специальном документе (например, матрице защиты). Доступ к системе ограничен операторами с документированным обучением.

229. Меры контроля для критически важных компонентов системы (например, серверов) включены и проверяются в процессе квалификации инфраструктуры.

Управление инцидентами

230. Инцидент – это любое незапланированное событие, которое не позволяет (или потенциально не позволяет) пользователям, системе, операции или службе выполнить запланированную задачу или задерживает ее выполнение. Инциденты собираются и управляются для совершения связанных действий, которые могут привести к немедленному локальному решению, запросу на изменение или CAPA.

231. Инциденты и разрешения на них должны отслеживаться в ходе мониторинга эффективности как процесса, так и автоматизированной системы, в рамках которой произошел инцидент. Это прослеживание обычно ведется в журнале инцидентов.

232. Процесс управления инцидентами предназначен для создания структуры высокого уровня, поддерживаемой подробными СОП, которые дают рекомендации по сценариям действий (эскалации и оценки) и связанными с ними инструментами. Этот процесс может поддерживаться программными средствами.

Управление изменениями

233. Управление изменениями применяется к компьютеризированным системам, подлежащим валидации на

протяжении всего жизненного цикла системы от этапа квалификации монтажа до вывода системы из использования

234. Управление изменениями использует процедуры контроля и информирования об изменениях, способных повлиять на элементы конфигурации (документация, аппаратное и программное обеспечение) и (или) валидированный статус системы. Управление изменениями включает отслеживание изменений (вызванных инцидентами или запросами на изменение) от их появления до их внедрения.

235. Процесс реализации изменений инициирует Управление конфигурацией, которое охватывает идентификацию, запись и отчетность об IT-компонентах, включая их версии, составляющие компоненты и отношения.

236. Изменения осуществляются в соответствии с заранее установленной процедурой управления изменениями.

Резервное копирование и восстановление

237. В соответствии с пунктами 118 – 120 настоящего Руководства, резервное копирование – это процесс копирования записей, данных и программного обеспечения для защиты от потери целостности или доступности оригинала. Восстановление – это последующее восстановление записей, данных или программного обеспечения при необходимости.

238. Данные процедуры необходимы для обеспечения восстановления основных систем в случае сбоев системы и последующей потери данных.

239. Надежность процесса восстановления должна быть проверена при валидации.

Соглашение об уровне обслуживания

240. С поставщиком и (или) интегратором GMP-систем среднего или высокого уровня, как правило, должно быть подписано Соглашение об уровне обслуживания (СУО), обеспечивающее адекватное и своевременное обслуживание при инцидентах, а также в целях надлежащего безопасного хранения документации системы, созданной во время разработки и хранящейся у поставщика.

241. Соглашение об уровне обслуживания определяет взаимную ответственность между регулируемой компанией и поставщиком вместе с соответствующими сроками.

Непрерывность деятельности

242. Процесс обеспечения непрерывности деятельности включает меры контроля, направленные на обеспечение непрерывности поддержки важнейших процессов в случае сбоя системы (например, ручная или альтернативная система).

243. Для каждой системы план обеспечения непрерывности деятельности содержит следующую информацию:

а) альтернативные процедуры на случай непредвиденных обстоятельств, используемые вместо этапов процесса, которые включают доступ к компьютеризированным системам;

б) планы управления и методы принятия решений, которые будут использоваться во время аварии (отказов) компьютеризированных систем;

в) идентификация важных с точки зрения непрерывности деятельности документов, которые необходимо временно хранить до восстановления работы компьютеризированных систем;

г) испытания процедур на случай непредвиденных обстоятельств.

244. Требование непрерывности деятельности считается строго применимым только для тех систем, которые поддерживают критически важные по времени процессы, то есть те системы, которые выполняют процессы, которые не могут быть прерваны без потенциального влияния на безопасность пациента, качество продукции и целостность данных. Необходимость наличия плана обеспечения непрерывности деятельности определяется в валидационном плане.

245. В качестве подмножества планов обеспечения непрерывности деятельности, должны быть разработаны, утверждены и отработаны планы восстановления конкретных систем в случае аварии. В этих планах необходимо подробно изложить меры, принимаемые для минимизации последствий аварии, что позволит организации либо сохранить, либо быстро возобновить выполнение важнейших функций. Особое внимание в плане аварийного восстановления уделяется предупреждению аварий (например, обеспечение резервирования для важнейших систем).

Архивирование

246. В случае, если данные архивируются в автономном режиме (то есть не сразу доступны пользователям), процедура архивирования определяет временные периоды и условия для архивирования данных. Процесс архивирования и восстановления данных должен быть задокументирован и проходить тестирование в течение жизненного цикла.

Периодический обзор

247. Валидационный статус каждой GMP-системы периодически проверяется для того, чтобы обеспечить поддержание валидированного состояния. Периодичность и глубина периодических проверок определяются на основе анализа рисков, связанных с системой.

248. Планирование периодических проверок включается в валидационный мастер план.

249. Периодические обзоры осуществляются в соответствии с заранее установленной процедурой.

Обучение и процедуры по использованию системы

250. Для каждой GMP системы должны быть разработаны обязательные для выполнения стандартных операционных процедур, определяющие порядок работы с системой и поэтапное выполнение операций. Кроме того, такие процедуры должны содержать раздел, посвященный специальным, а не рутинным действиям, соответствующим каждой системе, таким как:

а) добавление, изменение и удаление записей;

б) выполнение рутинных периодических задач (например, перестроение индекса базы данных);

в) подготовка (выбор и сортировка, определение последовательностей и т д.) экранных запросов и распечатанных отчетов о системных данных;

г) запуск управляемых пользователем интерфейсов передачи данных в другие системы и из других систем;

д) выгрузка или загрузка данных на рабочую станцию или устройства удаленного сбора данных из системы;

е) проверка контрольного следа.

251. Учебные планы и учебные записи должны поддерживаться для того, чтобы продемонстрировать аудиторам, что системы используются квалифицированным и обученным персоналом.

9. Особые указания по валидации

Валидация глобальных систем

252. Глобальные системы – это IT-системы, которые централизованно управляются и используются на нескольких площадках регулируемой компании; эти системы могут быть централизованно внедрены и введены в эксплуатацию или распространены для использования на каждой площадке. Для этих систем жизненный цикл валидации, рассматриваемый в рамках этой процедуры, может быть скорректирован таким образом, чтобы обеспечить максимально централизованное создание согласованной документации и свести к минимуму усилия по валидации на уровне площадки.

253. Для каждой глобальной системы подход к валидации определяется в едином глобальном плане валидации, который определяет глобальные и локальные результаты. Локальная реализация может быть детализирована в плане проверки конкретной площадки, созданном в соответствии с вышеупомянутым глобальным валидационным планом.

254. Процесс валидации для этих систем может включать глобальный пакет валидации, ориентированный, в первую очередь, на обеспечение функциональной надежности системы. Каждая площадка может официально принять результат глобальной валидации и создать

локальную спецификацию (документацию) по тестированию, связанную с функциональными возможностями площадки, если таковые имеются. Процесс валидации должен включать в себя верификацию процессов, выполняемых посредством системы на каждой отдельной площадке.

255. Глобальная документация должна быть доступна для площадки в случае проведения инспекции. Локальный подход площадки к валидации должен утверждаться глобальным руководством для обеспечения гармонизированного и согласованного подхода.

256. Локальная команда должна быть обучена, чтобы быть в курсе стратегии, используемой для проведения валидации на глобальном и локальном уровнях.

Валидация «облачных» систем

257. При использовании «облачных» или «виртуальных» сервисов необходимо уделять внимание пониманию предоставляемых услуг, владению, извлечению, хранению и безопасности данных.

258. Обязанности заказчика системы (то есть регулируемой компании) и исполнителя (поставщика IT-услуг) определяются техническим соглашением или договором. Соглашение должно обеспечивать своевременный доступ к данным (включая метаданные и контрольные журналы) владельцу данных и национальным компетентным органам по запросу. Контракты с поставщиками определяют ответственность за архивирование и непрерывную читаемость данных в течение всего периода хранения.

259. В настоящее время регулируемым компаниям предоставляются следующие виды услуг:

а) программное обеспечение как услуга (Software-as-a-Service, SaaS) – регулируемые компании используют приложения, работающие

на инфраструктуре, принадлежащей поставщику IT-услуг. Регулируемые компании не управляют и не контролируют базовую инфраструктуру или даже отдельные возможности приложений, за исключением ограниченных пользовательских параметров конфигурации приложений;

б) платформа как услуга (Platform-as-a-Service, PaaS) – регулируемые компании используют IT-инфраструктуру, размещенную поставщиком IT-услуг, для запуска приложений, созданных с использованием операционных систем, языков программирования и инструментов, поддерживаемых поставщиком IT-услуг. Регулируемые компании не управляют и не контролируют базовую облачную инфраструктуру, включая сеть, серверы, операционные системы или хранилище, но по-прежнему контролируют развернутые приложения и, возможно, конфигурации среды размещения приложений;

в) инфраструктура как услуга (Infrastructure-as-a-Service, IaaS) – владелец использует основные вычислительные ресурсы, такие как обработка, хранение, сети, где клиент может развертывать и запускать произвольное программное обеспечение, которое может включать операционные системы и приложения. Клиент не управляет базовой облачной инфраструктурой, но имеет контроль над операционными системами, хранилищем, развернутыми приложениями и, возможно, ограниченный контроль над выбранными сетевыми компонентами (например, брандмауэрами хоста).

260. Надежность компьютеризированной системы, используемой регулируемой компанией, всегда находится в зоне ответственности регулируемой компании, которая должна документировать соответствующий процесс валидации, используя документацию, предоставленную поставщиком системы.

261. Жизненный цикл валидации осуществляется в соответствии с изложенным в предыдущих разделах, гарантируя, что следующие конкретные меры должным образом проверены (подтверждены):

а) оценка поставщика выполнена на месте и до определения стратегии валидации в плане валидации; метод оценки поставщика должен основываться на риске, связанном с системой;

б) план валидации учитывает результаты этапа оценки поставщика;

в) документация по валидации может использовать спецификации, документацию по квалификации монтажа (IQ) и функционирования (OQ), предоставленную поставщиком, если эти документы будут признаны адекватными при оценке поставщика;

г) эффективный статус соглашения об уровне обслуживания проверен на этапе тестирования IQ;

д) квалификация эксплуатации (PQ) (Приемочный тест пользователя (User Acceptance Test UAT)) выполняется конечным пользователем регулируемой компании, проверяющим, что система работает по назначению пользователя (на основе спецификации требований пользователей) во всех предполагаемых рабочих диапазонах.

262. Выбор систем должен осуществляться на основе надежной оценки поставщиков по всем аспектам предоставляемых услуг. Допускается привлекать консультантов, обладающих знаниями в области IT, для эффективного тестирования «облачного» программного обеспечения, платформы и инфраструктуры, а также для проверки соответствия и управляемости «облачного» приложения. Аудит IT-безопасности должен быть ориентирован как минимум на следующие аспекты:

а) как поставщик уведомляет регулируемую компанию о проблемах, которые влияют на целостность данных, включая, но не ограничиваясь, следующими из них: технические ошибки и ошибки хостинга, ошибки, связанные с нарушениями защиты, ошибки в программном обеспечении, проблемы резервного копирования и восстановления и (или) выполнения плана аварийного восстановления;

б) безопасность авторизации и требования по разделению обязанностей;

в) процесс управления изменениями для улучшений, исправлений, обновлений;

г) на требования к хранению контрольного следа и журнала событий (Event Log);

д) механизм управления доступом;

е) механизм идентификации и аутентификации;

ж) механизм шифрования;

з) квалификация инфраструктуры (даже если инфраструктура управляется третьей стороной);

и) пакет валидации (спецификация и протоколы тестирования). Любые обнаруженные пробелы (несоответствия) должны быть устранены посредством корректирующих действий, согласованных Поставщиком, и дополнительных мероприятий по валидации в рамках проекта внедрения (например, дополнительных испытаний), выполняемых регулируемой компанией.

263. «Облачные» приложения рассматриваются только как соответствующие категориям 4 или 5 по классификации категорий компьютеризированных систем, указанной в пункте 153. С точки зрения регулируемой организации конфигурация облачных приложений, должна рассматриваться как категория 4, в то же время любая

пользовательская разработка интерфейсов или передачи данных, влияющих на GMP, связанная облачным приложением, должна рассматриваться как соответствующая категория 5 и должна быть испытана соответствующим образом.

264. Если «облачная» инфраструктура (IaaS и PaaS) была выбрана для реализации, необходимо убедиться, что она соответствующим образом квалифицирована поставщиком и (или) регулируемой компанией в соответствии с пунктами 270 – 277 настоящего Руководства.

Валидация электронных таблиц

265. Каждая электронная таблица рассматривается в качестве одиночной компьютеризированной системы, и поэтому критические электронные таблицы подлежат инвентаризации, оценке риска и валидации соответственно.

266. Электронные таблицы обычно применяются для повторения алгоритма расчета; использование Excel в качестве базы данных (то есть электронная таблица, используемая для хранения и архивирования GMP-данных) не допускается, если контрольный след не отслеживается с помощью дополнительных мер.

267. Категория таблицы Excel по категоризации компьютеризированных систем, приведенной в пункте 153 зависит от типа операций, которые выполняются с GMP данными в этой таблице и определяется следующим:

а) категория 3 (не конфигурированная) – электронная таблица просто использует собственные функции без конфигурации (например, данные валидации, условное форматирование);

б) категория 4 (конфигурированная) – электронная таблица выполняет вычисления с помощью настроенных формул, а также формул, использующих основные функции Excel (например, сложение, вычитание, деление);

в) категория 5 (пользовательская) – электронная таблица использует пользовательские макросы, сложные или вложенные логические и схожие функции.

268. Каждая система электронных таблиц должна использоваться с учетом следующих факторов:

а) обеспечение безопасности электронной таблицы, гарантируя, что могут быть заполнены только входные ячейки (например, формулы не могут быть намеренно или случайно перезаписаны, параметры разработки отключены);

б) настройка безопасности доступа и проверки авторизации, например, создание электронной таблицу Excel в выделенной папке с правами доступа, определенными для всех пользователей электронной таблицы;

в) выполнение любых вычислений, связанных с точностью, отображаемой на экране и в отчетах;

г) использование переменных электронной таблицы, (в Microsoft Excel называемые «Именами»), дающих возможность создания формулы (например, вместо включения в формулу ссылки на ячейку A4, определить A4 именем «количество» и включить строку «Количество» в формулу);

д) обеспечение правильности выполнения резервного копирования (для электронных таблиц, хранящихся в локальных каталогах);

е) защищенность «привязки» ко времени, включая часовой пояс;

ж) проверка того, что заполненная таблица сохраняется в нередактируемом файле (например, в формате PDF);

з) при использовании таблицы как шаблона, настройка должна обеспечивать ее сохранение только в защищенной папке.

269. Результаты жизненного цикла валидации, описанные в пунктах 165 – 224 настоящего Руководства, должны быть созданы для каждой таблицы, при этом некоторые документы могут быть объединены вместе (например, единый документ, описывающий функциональные требования спецификации требований пользователей URS/FS).

10. Квалификация IT-инфраструктуры

270. IT-инфраструктура поддерживает сетевые системы, участвующие в производственной и управленческой деятельности предприятий компании. Для запуска валидированных приложений требуется квалифицированная инфраструктура.

271. Квалификация инфраструктуры обеспечивает документированную верификацию правильности работы и контролируемого статуса IT-инфраструктуры.

272. IT-инфраструктура существует для поддержки основной деятельности, предоставляя: платформу для запуска бизнес-приложений, процессы IT-инфраструктуры, которые облегчают пригодную и контролируемую IT-среду, общие IT-услуги (например, офисные инструменты, средства интрасети, хранилище файлов)

273. С процессом квалификации компонентов IT-инфраструктуры связаны следующие этапы:

а) планирования – для выполнения требуемых действий, обязанностей, процедур и сроков, гарантируя, что квалификационные

мероприятия выполняются систематическим и контролируемым образом, на основе предопределенной стратегии;

б) спецификации и создания проекта IT-инфраструктуры который подробно описывает аппаратную и программную структуру компонентов IT-инфраструктуры, подлежащих квалификации, гарантируя, что документация, связанная с IT-инфраструктурой, организована и интегрирована, чтобы быть легкоуправляемой и контролируемой;

в) тестирования, чтобы убедиться, что IT-инфраструктура обеспечивает надежную и точную работу;

г) отчетности по результатам квалификации для подведения итогов проведенных мероприятий по квалификации;

д) функционирования IT-инфраструктуры, чтобы гарантировать статус «квалифицировано».

274. Следующие виды деятельности жизненного цикла должны рассматриваться как обязательные для каждого компонента IT-инфраструктуры, относящегося к GMP:

а) оценка влияния на GMP;

б) план квалификации и отчетность;

в) проектная спецификация;

г) испытания при квалификации монтажа (IQ) и функционирования (OQ);

д) вспомогательные процессы;

е) управление изменениями;

ж) управление конфигурацией;

з) резервное копирование и восстановление;

и) защита инфраструктуры;

к) управление инцидентами.

275. Решение вышеперечисленных задач для GMP-компонентов позволяет обеспечить документально подтвержденное состояние контроля, необходимого для GMP IT-инфраструктуры. Документация, созданная в течение жизненного цикла, будет представлять собой квалификационную документацию по IT-инфраструктуре, которая содержит документальные доказательства надлежащей работы IT-инфраструктуры, документально подтверждая, что она управляется, как указано в применимых руководящих принципах.

276. Процесс квалификации IT-инфраструктуры, требуемый Правилами надлежащей производственной практики, следует осуществлять в соответствии со специальным планом.

277. Квалификация IT-инфраструктуры является необходимым предварительным условием валидации программного обеспечения, которая выполняется в IT-инфраструктуре.

VIII. Обеспечение целостности данных для аутсорсинговой деятельности

278. Целостность данных играет ключевую роль в обеспечении безопасности и целостности предоставляемых извне продуктов и услуг. Меры по управлению данными подрядчика могут быть значительно ослаблены ненадежными или фальсифицированными данными, предоставленными другими партнерами по цепочке поставок. Это относится ко всем видам деятельности, переданным на аутсорсинг, включая поставщиков сырья, контрактное производство или контрольно-аналитические услуги.

279. Первоначальная и периодическая реквалификация поставщиков и аутсорсинговой деятельности должны включать учет рисков целостности данных и соответствующие меры контроля.

280. Важно, чтобы организация понимала ограничения целостности данных, полученных от поставщика (например, краткие отчеты и копии (распечатки)), а также сложности дистанционного надзора. Обычно необходимым является дистанционный анализ данных в сводных отчетах, однако ограничения дистанционного анализа данных должны быть полностью поняты, чтобы обеспечить надлежащий контроль целостности данных.

281. Важно, чтобы краткие отчеты рассматривались как передача данных, и чтобы заинтересованные стороны не полагались исключительно на данные кратких отчетов. До принятия сводных данных, оценка системы качества поставщика и соблюдение принципов целостности данных должны быть установлены путем аудита на площадке поставщика. Аудит должен дать уверенность в достоверности данных, генерируемых компанией-подрядчиком, и включать обзор механизмов, используемых для формирования и передачи сводных данных и отчетов.

282. Следует проводить регулярные обзоры рисков, связанных с поставщиками и аутсорсинговой деятельностью, периодически оценивая степень требуемых мер контроля в отношение целостности данных.

283. Между регулируемыми компаниями и поставщиками (подрядными) организациями (например, контрактными производителями) должны быть заключены соглашения по качеству, содержащие конкретные положения по обеспечению целостности данных в рамках поддерживаемого процесса (процессов). Это может быть достигнуто путем формирования ожиданий в области управления данными, а также путем обеспечения «прозрачности» относительно отчетности Исполнителя перед Заказчиком на предмет ошибок

(отклонений). Также должно быть установлено требование о немедленном информировании Заказчика о каких-либо сбоях целостности данных, произошедших на стороне Исполнителя. Аудиты поставщиков (в том числе, поставщиков услуг), проводимые производителем (или третьей стороной от имени производителя), должны включать проверку мер по обеспечению целостности данных в контрактной организации.

IX. Регуляторные меры в ответ на несоответствия, выявленные в области целостности данных

284. Несоответствия, обусловленные нарушением целостности данных, могут по-разному влиять на качество продукции. «Обширность» сбоя также может варьировать от действий одного сотрудника до сбоя в рамках всей инспектируемой организации.

285. В случае обнаружения нарушения целостности данных, в первую очередь, следует рассмотреть возможность разрешения выявленных проблем и оценки рисков, связанных с проблемами целостности данных, а также ретроспективной оценки данных. В ответе со стороны регулируемой компании на выявленные несоответствия должны быть изложены принятые меры.

286. Регулируемой компании следует провести детальное расследование, включая обзор всех задействованных лабораторий, производственных операций и систем, а также обоснование любой части операции, которую регулируемый пользователь предлагает исключить. В ходе расследования могут проводиться собеседования с нынешними и бывшими сотрудниками компании для выявления характера, масштабов и корневых причин неточностей в данных. Эти

собеседования могут проводиться квалифицированной третьей стороной.

287. Расследование включает в себя оценку, которая должна установить:

а) масштаб нарушения целостности данных на объекте, не ограничиваясь одним наблюдаемым случаем, а проверяя все другие случаи, когда нарушение могло произойти;

б) влияние нарушения целостности данных на безопасность пациента и качество продукции, определяемое с учетом рисков, связанных с текущими операциями, и любое влияние на достоверность данных, представленных в регуляторные органы, включая данные, связанные с регистрационными досье на продукцию;

в) выявление корневых причин нарушения целостности данных.

288. Корректирующие и предупреждающие действия, предпринятые для устранения уязвимостей целостности данных, и сроки их реализации включают в себя, но не ограничиваются этим:

временные меры, описывающие действия по защите пациентов и обеспечению качества лекарственных средств, (например, уведомление клиентов, отзыв продукции, проведение дополнительного тестирования, включение серий продукции в программу последующего изучения стабильности, действия в отношение регистрационного досье и усиленный мониторинг поступающих рекламаций (претензий));

долгосрочные меры, включающие действия по восстановлению и усовершенствованию процедур, процессов, методов, средств контроля, систем, управленческого надзора и методов управления персоналом (например, обучение, кадровые усовершенствования), предназначенные для обеспечения целостности данных.

X. История изменений

289. Историю изменений следует оформлять в виде таблиц, согласно приведенной форме.

Форма таблицы истории изменений

Дата введения	Номер редакции	Содержание изменения
	01	Введение нового документа