Приложение 11

Компьютеризированные системы

Основные принципы

Данное приложение применяется ко всем типам компьютеризированных систем, используемых в области применения настоящего стандарта. Компьютеризированная система представляет собой набор программных компьютерное оборудование, которые совместно выполняют определенные функции.

Применение компьютеризированной системы и информационно-технологическая инфраструктура должны быть аттестованы.

Если компьютеризированная система заменяет ручное управление, это не должно приводить к снижению качества продукции, технологического контроля или обеспечения качества. Общий риск процесса не должен возрастать.

Общие положения

1 Анализ рисков

Анализ рисков должен выполняться в течение жизненного цикла компьютеризированной системы в целях обеспечения безопасности пациентов, целостности данных и качества продукции. Решения по объему испытаний и контролю целостности данных должны основываться на обоснованной и документально оформленной оценке рисков компьютеризированной системы.

2 Персонал

Следует организовать взаимодействие между всеми лицами, имеющими отношение к данному процесс, включая владельцев процесса и системы, уполномоченных лиц и информационно-технологический персонал. Весь персонал должен иметь необходимую квалификацию, уровень доступа и нести ответственность за выполнение своих обязанностей.

3 Поставщики продукции и услуг

3.1 Если для поставки, установки, наладки, задания конфигурации, интегрирования, аттестации, технического обслуживания (в том числе через удаленный доступ), модификации или поддержания компьютеризированных систем, оказания связанных с ними услуг или обработки данных привлекаются третьи лица (в частности, поставщики продукции и услуг), то между производителем и указанными третьими лицами заключаются договоры. Такие договоры должны предусматривать ответственность третьих лиц за выполнение своих обязанностей. Аналогичные требования предъявляются к информационно-технологическим подразделениям.

3.2 Основными требованиями к поставщикам продукции или услуг являются их компетентность и надежность. Необходимость в аудите рекомендуется определять с использованием оценки рисков.

3.3 Документация, прилагаемая к коммерчески доступным готовым для использования программным продуктам, должна быть рассмотрена пользователями, которые подлежат контролю, на предмет соответствия требованиям производителя.

3.4 Информация о системе качества и аудитах поставщиков или разработчиков программного обеспечения и установленных систем должна быть доступна для предоставления лицам, осуществляющим контроль, по их требованию.

Стадия разработки

4 Аттестация

4.1 Документация аттестации я и отчеты должны охватывать соответствующие стадии жизненного цикла компьютеризированной системы. Производитель должен обосновать свои стандарты, протоколы, критерии приемлемости, инструкции и записи на основе оценки рисков.

4.2 Документация по аттестации должна включать протоколы контроля изменений (если требуется) и отчеты о любых отклонениях, выявленных при аттестации.

4.3 Следует иметь действующий перечень (реестр) всех используемых компьютеризированных систем с указанием их функций в рамках области применения настоящего стандарта.

Для критических систем следует иметь подробное действующее описание физических и логических взаимосвязей, потоков данных и интерфейсов с другими системами или процессами, данные о всем компьютерном оборудовании и программном обеспечении и мер безопасности.

4.4 Спецификации требований пользователя (задание на разработку) должны описывать необходимые функции системы на основе документально оформленной оценки рисков и соблюдения настоящего стандарта. Требования пользователя должны прослеживаться в течении всего жизненного цикла системы.

4.5 Пользователь должен предпринять все меры, гарантирующие, что компьютеризированная система разработана в соответствии с системой обеспечения качества. Поставщик должен быть оценен соответствующим образом.

4.6 Для аттестации компьютеризированных систем, разработанных по индивидуальному заказу или модифицированных в соответствии с требованиями заказчика, необходимо разработать методику оценки качества и эксплуатационных характеристик системы на всех этапах ее жизненного цикла с оформлением соответствующих отчетов.

4.7 Следует предоставить свидетельства соответствия методик контроля и тестирования. В частности, следует пределы параметров системы (процесса), границы данных и действия в случае ошибок. Необходимо документально оформить оценку соответствия автоматизированных средств тестирования и режимов их работы.

4.8 Если данные переводятся в другой формат или систему данных, то аттестация должна включать проверку неизменности значения и/или смысла данных в процессе их переноса.

Стадия эксплуатации

5 Данные

Компьютеризированные системы, осуществляющие электронный обмен данных с другими системами, должны иметь соответствующие встроенные средства контроля правильного и безопасного ввода и обработки данных с целью минимизации рисков.

6 Контроль точности

Для критических данных, вводимых вручную, необходимо предусмотреть дополнительный контроль точности ввода данных. Этот контроль может осуществляться вторым оператором или с помощью аттестованных электронных средств. Критичность и возможные последствия ошибок или неправильного ввода данных в систему должны быть учтены при анализе рисков.

7 Хранение данных

7.1 Следует защищать от искажений как физическими, так и электронными мерами. Следует проверять доступность, читаемость и точность сохраненных данных. Доступ к данным должен быть обеспечен на протяжении всего периода их хранения.

7.2 Следует выполнять регулярное резервное копирование всех необходимых данных. Сохранность и точность резервных копий, а также возможность восстановления данных должны быть проверены в процессе аттестации и периодически контролироваться.

8 Распечатки

8.1 Следует иметь возможность получения четких печатных копий данных, хранящихся в электронном виде.

8.2 Для записей, сопровождающих разрешение на выпуск серии, должна быть предусмотрена возможность получения распечаток, указывающих, изменялись ли какие-либо данные с момента их первоначального ввода.

9 Контрольные следы

Следует предусмотреть внесение в систему записей всех существенных изменений и удалений, связанных с применением настоящего стандарта (система, создающая «контрольные следы»), прибегая к анализу рисков. Следует таких документально оформлять причины изменений или удалений Контрольные следы должны быть доступными, должна быть возможность их преобразования в понятную для пользователей форму, их следует регулярно рассматривать.

10 Внесение изменений и изменение конфигурации

Любые изменения в компьютеризированной системе, включая конфигурацию системы, должны проводиться только контролируемым способом в соответствии с инструкцией.

11 Периодическая оценка

Следует периодически оценивать компьютеризированные системы ля подтверждения того, что они соответствуют результатам и настоящему стандарту. При этом следует, где требуется, оценивать текущие функциональные возможности, данные об отклонениях, сбоях, проблемах, истории обновлении, отчеты об эксплуатации, надежности, защищенности и о проведении аттестации.

12 Безопасность

12.1 Следует предусмотреть физические и логические средства защиты для ограничения доступа к компьютеризированной системе только лиц, имеющими на это право. Средства для предотвращения несанкционированного доступа к системе могут включать в себя использование ключей, карточек доступа, персональных кодов с паролями, биометрических данных, ограничения доступа к компьютерному оборудованию и зонам хранения данных.

12.2 Степень защиты зависит от критичности компьютеризированной системы.

12.3 Создание, изменение и аннулирование прав доступа должно быть оформлено докумен-

тально.

12.4 Следует разработать систему контроля данных и документов для идентификации операторов, которые входят в систему, и для регистрации изменения, подтверждения или удаления данных, включая дату и время.

13 Действия при сбоях в работе

Следует регистрировать и анализировать все сбои в работе, включая системные сбои и ошибки данных. Необходимо установить основную причину критических сбоев и использовать эту информацию в качестве основы корректирующих и предупреждающих действий.

14 Электронная подпись

Документы в электронной форме могут быть заверены электронной подписью. Электронные подписи должны:

a) в рамках организации иметь ту же силу, что и подписи от руки;

b) быть неразрывно связанными с соответствующими документами;

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

15 Выпуск серии

В случаях, когда выпуск серии продукции осуществляется с использованием компьютеризированной системы, она должна предоставлять доступ для выпуска серии только уполномоченному лицу и четко идентифицировать и регистрировать уполномоченное лицо, которое одобрило и выпустило серию. Эти действия должны осуществляться с использованием электронной подписи.

16 Непрерывность работы

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

17 Архивирование данных

В случае необходимости архивирования данные следует проверять на доступность, удобство чтения и целостность. Если в компьютеризированной системе необходимо провести существенные изменения (например, компьютерного оборудования или программного обеспечения), следует обеспечить и проверить возможность восстановления данных.

Термины и определения

Владелец процесса (process owner): лицо, ответственное за рабочий процесс;

Владелец системы (system owner): лицо, ответственное за доступ и техническое обслуживание компьютеризированной системы и безопасности данных, находящихся в этой системе;

Жизненный цикл (life cycle): все стадии существования компьютеризированной системы от постановки задачи до прекращения эксплуатации, включая задание исходных требований разработку, программирование, тестирование, установку, пользование и обслуживание;

Информационно-технологическая инфраструктура (IT Infrastructure): компьютерное оборудование и программное обеспечение, такое как сетевые и операционные системы, которые позволяют применять их для выполнения определенных функций;

Компьютеризированная система, изготовленная по индивидуальному заказу (bespoke/customized computerized system): индивидуально разработанная компьютеризированная система для обеспечения конкретного процесса;

Приложение (application): программное обеспечение, установленное на определенной платформе или компьютерном оборудовании и выполняющее специальные функции;

Серийное программное обеспечение (commercial off the shelf software): коммерчески доступное программное обеспечение, пригодность которого для использования продемонстрирована большим количеством пользователей.