IV. Стадия эксплуатации

Данные (5)

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

Контроль точности (6)

21. Для критических данных, вводимых вручную, необходимо предусмотреть дополнительный контроль точности ввода данных. Этот контроль может осуществляться вторым оператором или с помощью валидированных электронных средств. Критичность и потенциальные последствия ошибочного или неправильного ввода данных в систему должны охватываться системой управления рисками.

Хранение данных (7)

22. (7.1) Данные должны быть защищены от повреждений как физическими, так и электронными мерами. Сохраненные данные должны проверяться на доступность, читаемость и точность. Доступ к данным должен быть обеспечен на протяжении всего периода их хранения.

23. (7.2) Необходимо выполнять регулярное резервное копирование всех необходимых данных. Сохранность и точность резервных копий, а также возможность восстановления данных должны быть проверены в процессе валидации и периодически контролироваться.

Распечатки (8)

24. (8.1) Необходимо иметь возможность получения четких печатных копий данных, хранящихся в электронном виде.

25. (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.

Контрольные следы (9)

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

Управление изменениями и конфигурацией (10)

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

Периодическая оценка (11)

28. Компьютеризированные системы должны периодически оцениваться для подтверждения того, что они остаются в валидированном состоянии и соответствуют требованиям настоящих Правил. Такие оценки должны включать, в случае необходимости, оценку текущего диапазона функциональных возможностей, записей отклонений, сбоев, проблем, истории обновлении, отчеты об эксплуатации, надежности, защищенности и о валидационном статусе.

Защита (12)

29. (12.1) Для обеспечения доступа к компьютеризированной системе только лицами, имеющими на это право, необходимо использовать физические и (или) логические элементы контроля. Соответствующие способы предотвращения несанкционированного доступа к системе могут включать в себя использование ключей, карточек доступа, персональных кодов с паролями, биометрических данных, ограничения доступа к компьютерному оборудованию и зонам хранения данных.

30. (12.2) Степень защиты зависит от критичности компьютеризированной системы.

31. (12.3) Создание, изменение и аннулирование прав доступа должно быть зарегистрировано.

32. (12.4) Должна быть разработана система управления данными и документами для идентификации операторов, осуществляющих вход, а также для регистрации изменения, подтверждения или удаления данных, включая дату и время.

Управление инцидентами (13)

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

Электронная подпись (14)

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

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

б) (b) быть неразрывно связанными с соответствующими записями;

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

Выпуск серии (15)

35. Если для регистрации процедуры одобрения и выпуска серии используется компьютеризированная система, она должна предоставлять доступ для выпуска серии только уполномоченному лицу, а также должна четко идентифицировать и регистрировать уполномоченное лицо, которое одобрило и выпустило серию. Эти действия должны осуществляться с использованием электронной подписи.

Непрерывность работы (16)

36. 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 альтернативной системы). Время, необходимое для введения в действие альтернативных средств, должно учитывать риски и соответствовать конкретной компьютеризированной системе и сопровождаемому рабочему процессу. Эти меры должны быть надлежащим образом оформлены документально и проверены.

Архивирование (17)

37. Данные могут архивироваться. Эти данные должны проверяться на доступность, удобство чтения и целостность. Если в компьютеризированной системе необходимо провести существенные изменения (например, компьютерного оборудования или программного обеспечения), должна быть обеспечена и проверена возможность восстановления данных.