ВАЛИДАЦИЯ КОМПЬЮТЕРИЗИРОВАННЫХ СИСТЕМ – ТАБЛИЦЫ EXCEL: РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД И ПРАКТИКА ВАЛИДАЦИИ НА ПРИМЕРАХ.

Нормативные требования евразийских правил GMP и регуляторные ожидания в отношении валидации компьютеризированных систем. Анализ инспекционной практики: разбор наиболее частых несоответствий.

Рыбаков Егор Владимирович

Заместитель генерального директора
по аудиторской деятельности
ООО «ФАРМСТРАТЕГИЯ»

Подготовлено компанией ФАРМСТРАТЕГИЯ по заказу ЕВРАЗИЙСКОЙ АКАДЕМИИ НАДЛЕЖАЩИХ ПРАКТИК в рамках совместной программы содействия технологическому развитию и повышению качества фармацевтического производства в странах – членах Евразийского экономического сообщества.

ФАРМСТРАТЕГИЯ

Р-ФАРМ
Инновационные технологии здоровья

НОРМАТИВНЫЕ ТРЕБОВАНИЯ ЕВРАЗИЙСКИХ ПРАВИЛ GMP И РЕГУЛЯТОРНЫЕ ОЖИДАНИЯ В ОТНОШЕНИИ ВАЛИДАЦИИ КОМПЬЮТЕРИЗИРОВАННЫХ СИСТЕМ

Должна быть разработана и утверждена Политика в области целостности данных, основанная на принципах Надлежащей практики документирования (GDocPS), а также ALCOA.

В соответствии с принципами ALCOA данные должны быть:

1. прослеживаемыми (Attributable);
2. читаемыми (Legible);
3. своевременными (Contemporaneous);
4. подлинными (Original);
5. точными (Accurate).

Политика в области целостности данных должна распространятся не только на данные полученные при использовании компьютеризированных систем, но также и на все записи.

Применение компьютеризированной системы должно быть валидировано, информационно-технологическая инфраструктура должна пройти квалификацию.

Если компьютеризированная система заменяет ручное управление, это не должно приводить к снижению качества продукции, технологического контроля или обеспечения качества. Общие риски процесса не должны возрастать.

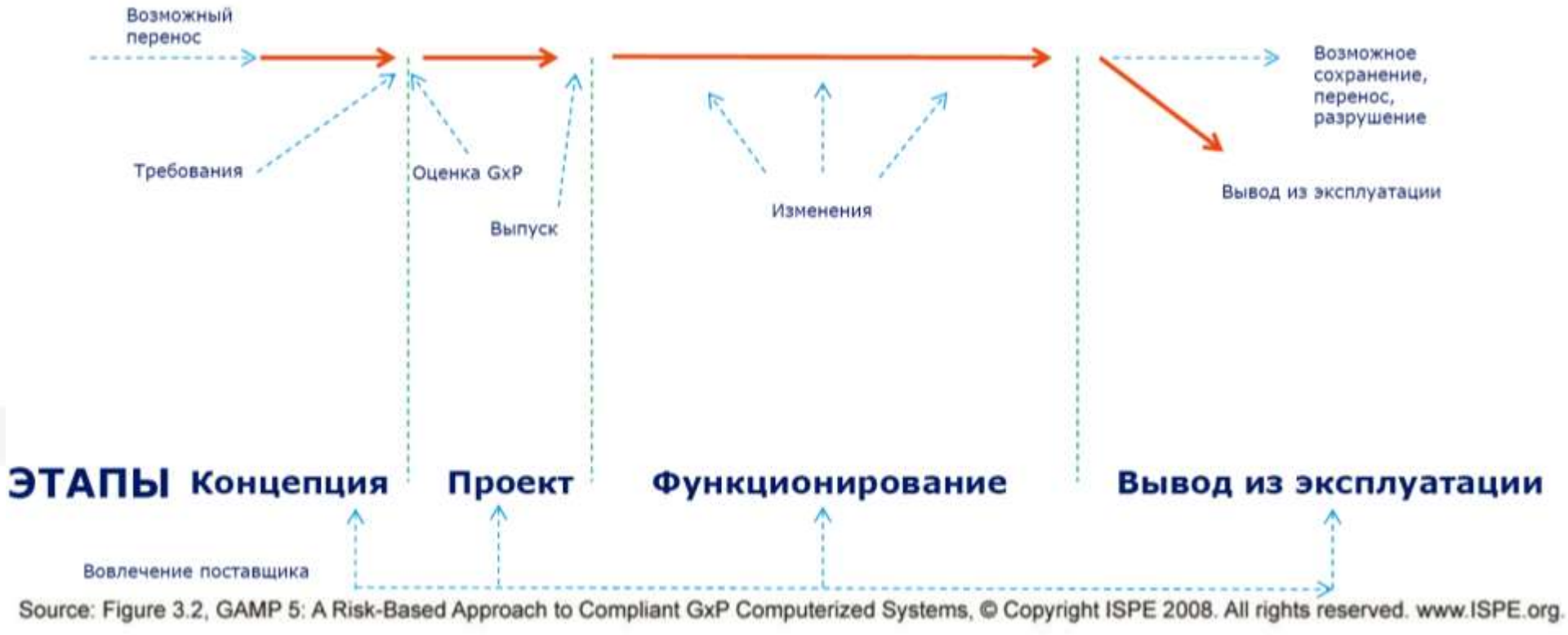
К информационно-технологической инфраструктуре относится:

- Внешние и локальные сети;
- Автоматизированные рабочие места (АРМ);
- Сетевые хранилища, в том числе облачные;
- Серверы, в том числе виртуальные;
- Периферийное офисное оборудование;
- Беспроводное сетевое оборудование.

- Управление рисками должно применяться в течение жизненного цикла компьютеризированной системы и учитывать безопасность пациентов, целостность данных и качество продукции.

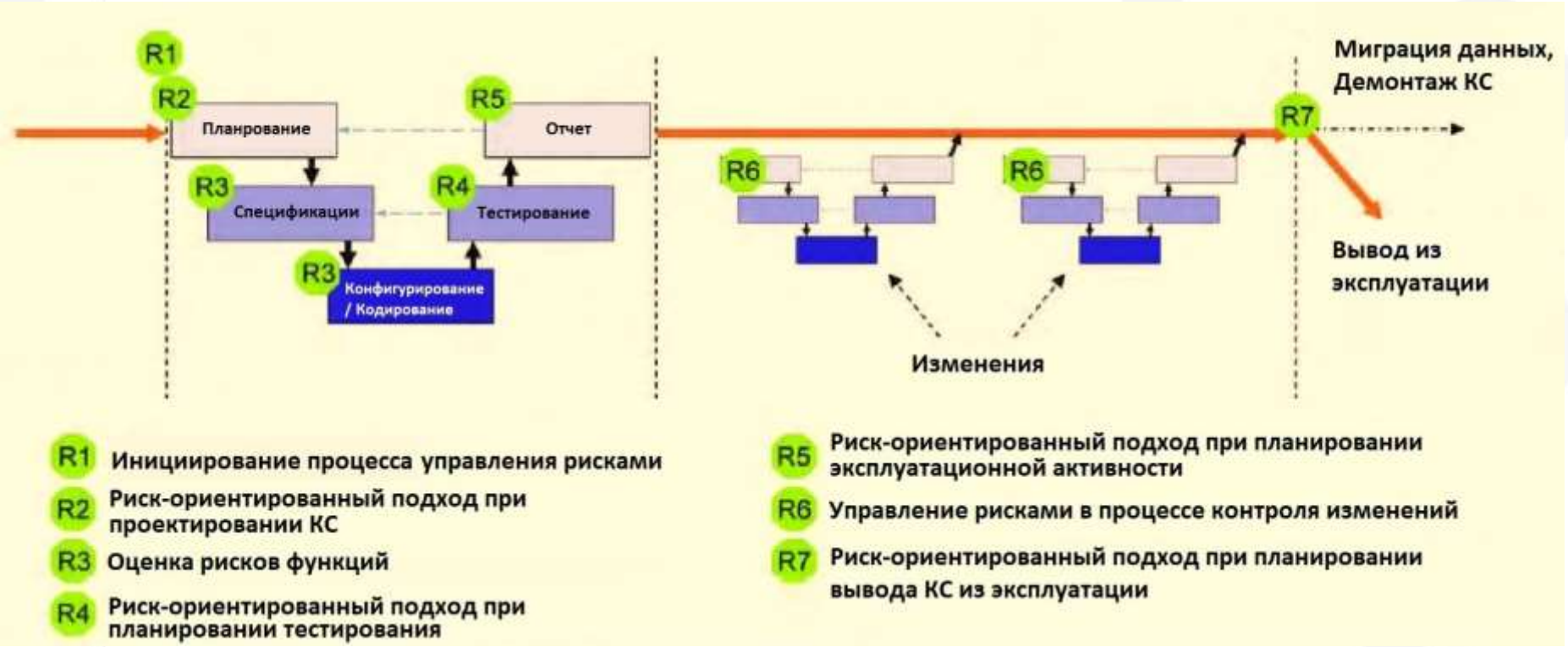
- В рамках системы управления рисками решения по объему валидационных испытаний и проведению контролей целостности данных должны основываться на обоснованной и документально оформленной оценке рисков компьютеризированной системы.

Жизненный цикл компьютеризированной системы



Source: Figure 3.2, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.

Управление рисками



- **R1** Инициирование процесса управления рисками
- **R2** Риск-ориентированный подход при проектировании КС
- **R3** Оценка рисков функций
- **R4** Риск-ориентированный подход при планировании тестирования
- **R5** Риск-ориентированный подход при планировании эксплуатационной активности
- **R6** Управление рисками в процессе контроля изменений
- **R7** Риск-ориентированный подход при планировании вывода КС из эксплуатации

Поставщики и провайдеры услуг.

- Должны быть заключены договора, в которых должна быть четко установлена ответственность третьих лиц;
- Поставщики должны быть утверждены;
- Необходимость аудита поставщика должна быть основана на анализе рисков;
- Вся поставляемая документация должна быть рассмотрена производителем на предмет своего соответствия требованиям пользователя;
- Информация о системе качества и аудитах поставщиков или разработчиков программного обеспечения и установленных компьютеризированных систем должна быть доступна для предоставления инспекторам по их требованию.

Валидация. Этапы валидации компьютеризированных систем

Планирование Валидации

- Идентификация проекта
- Оценка проекта
- Планирование валидации

Квалификация

- Квалификация проекта
- Квалификация инсталляции
- Квалификация функционирования (Тестирование)

Выпуск

- Сводные отчеты по всем этапам валидации

- 4.1 Валидационная документация и отчеты должны охватывать соответствующие стадии жизненного цикла компьютеризированной системы.
- Производители должны быть способны обосновать свои стандарты, протоколы, критерии приемлемости, процедуры и записи на основе оценки рисков.
- 4.2 Валидационная документация должна включать в себя записи контроля изменений (если применимо) и отчеты о любых отклонениях, выявленных в ходе процесса валидации.
- 4.3 Должен быть в наличии текущий перечень (реестр) всех используемых компьютеризированных систем с указанием их функциональности, регулируемой требованиями Правил.

- 4.5. Заказчику следует предпринять все меры, гарантирующие, что компьютеризированная система разработана в соответствии с надлежащей системой управления качеством.
- Поставщик должен быть оценен соответствующим образом.
- 4.7. Следует представить доказательства соответствия методов и схем тестирования компьютеризированной системы. В частности, должны быть рассмотрены пределы параметров системы (процесса), границы данных и обработка ошибок. Следует документально оформить оценку соответствия применения автоматизированных средств тестирования и режимов их работы.
- 4.8. Если данные переводятся в другой формат или систему данных, валидация должна включать проверку неизменности значения и смысла данных в процессе их миграции.

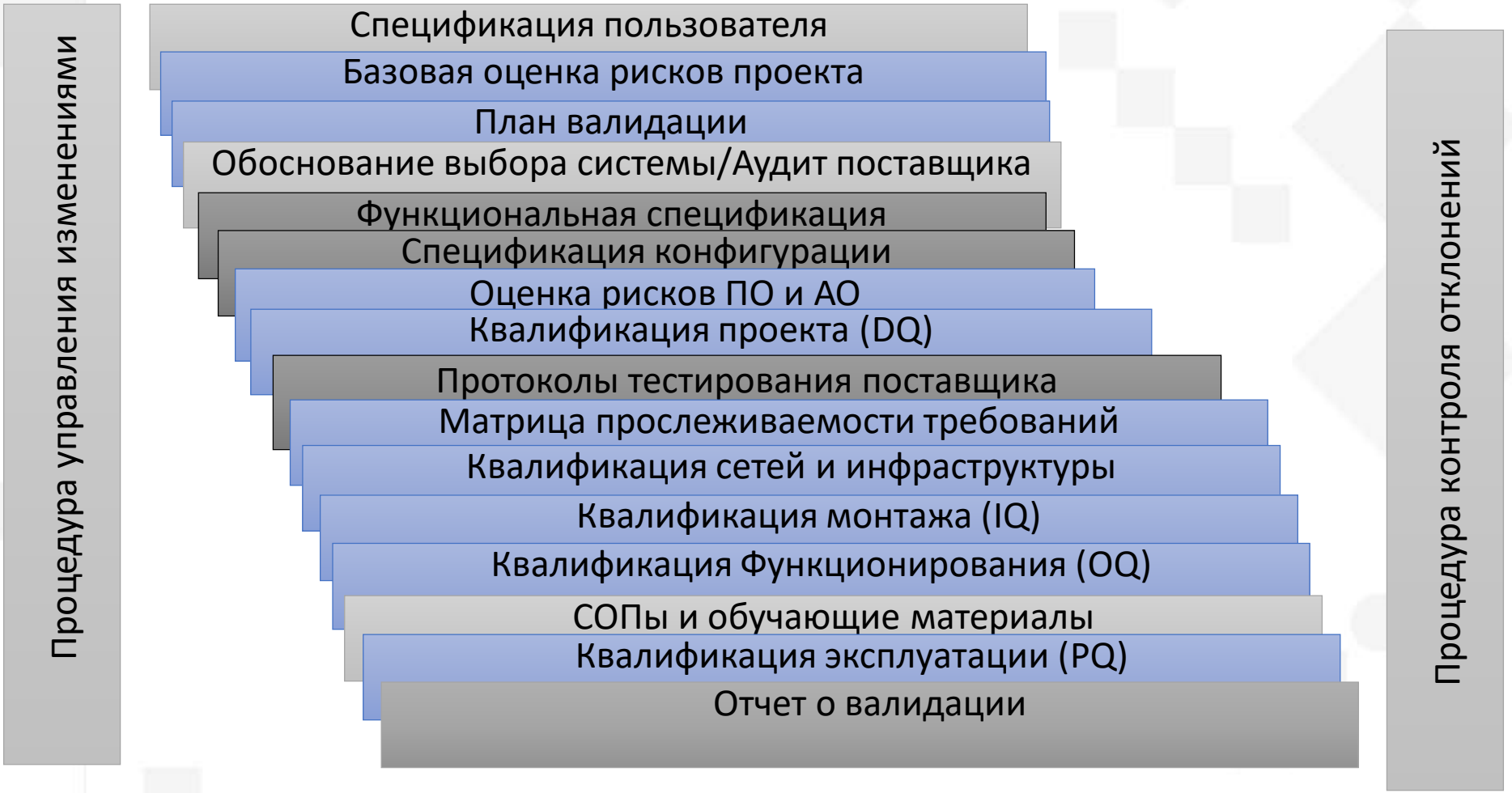
- Для критических данных, вводимых вручную, следует предусмотреть дополнительный контроль точности ввода данных. Этот контроль может осуществляться вторым оператором или с помощью валидированных электронных средств. Критичность и потенциальные последствия ошибочного или неправильного ввода данных в систему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

- 8.1. Необходимо иметь возможность получения четких печатных копий данных, хранящихся в электронном виде.
- 8.2. Для записей, сопровождающих разрешение на выпуск серии, следует предусмотреть возможность получения распечаток, указывающих, изменялись ли какие-либо данные с момента их первоначального ввода.
- На основе оценки рисков следует уделить внимание встраиванию в систему возможности создания записей всех существенных изменений и удалений, связанных с областью действия Правил (система, создающая «контрольные следы»). Причины таких связанных с 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.

- Компьютеризированные системы должны периодически оцениваться для подтверждения того, что они остаются в валидированном состоянии и соответствуют требованиям Правил. Такие оценки должны включать, в случае необходимости, оценку текущего диапазона функциональных возможностей, записей отклонений, сбоев, проблем, истории обновлении (upgrades), отчеты об эксплуатации, надежности, защищенности и о валидационном статусе.
- 12.1. Должны иметься в наличии физические и (или) логические элементы контроля для обеспечения доступа к компьютеризированной системе только уполномоченным на то лицам.
- 12.2. Степень защиты зависит от критичности компьютеризированной системы.
- 12.3. Создание, изменение и аннулирование прав доступа должно быть зарегистрировано.

- 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 сотрудника, который одобрил и выпустил серию в реализацию. Эти действия должны осуществляться с использованием электронной подписи.

МИНИМАЛЬНЫЙ ПАКЕТ ВАЛИДАЦИОННОЙ ДОКУМЕНТАЦИИ



ФАРМСТРАТЕГИЯ

Р-ФАРМ
Инновационные технологии здоровья

КАТЕГОРИЗАЦИЯ НЕСООТВЕТСТВИЙ

КАТЕГОРИЗАЦИЯ НЕСООТВЕТСТВИЙ СОГЛАСНО РЕШЕНИЮ ЕЭК №77 ОТ 03.11.2016

Критические <*> Несоответствия, которые вызывают или приводят к существенному риску возможности производства лекарственного средства, опасного для здоровья и жизни человека.

Существенные <>** Несоответствия, которые не могут классифицироваться как критические, но:

- привели к производству или могут привести к производству лекарственного средства, не соответствующего документам регистрационного досье данного лекарственного препарата;
- указывают на существенное отклонение от правил надлежащей производственной практики Евразийского экономического союза;
- указывают на существенное отклонение от требований иных актов законодательства в сфере обращения лекарственных средств;
- указывают на неспособность инспектируемого субъекта осуществлять серийный выпуск лекарственных препаратов однородного качества или неспособность уполномоченного лица инспектируемого субъекта выполнять свои должностные обязанности;
- комбинация несоответствий, ни одно из которых само по себе не является существенным, но которые в совокупности представляют существенное несоответствие и должны объясняться и фиксироваться в качестве такового.

Прочие <*>** Несоответствия, которые не могут классифицироваться как критические или существенные, но указывают на отклонение от требований правил надлежащей производственной практики, утверждаемых Евразийской экономической комиссией.

- Подробная оценка несоответствия для определения первичной классификации
- Оценка факторов, которые либо повышают, либо снижают риск, вне зависимости от первичной классификации
- Принятие решения о том, как поступить с первичной классификацией риска:
  - повысить по причине влияния, повышающего риск
  - сохранить или
  - понизить по причине влияния, снижающего риск

Факторы, которые учитываются при категоризации несоответствий:

- риск для здоровья и безопасности пациента
- история соответствия производителя
- действовал ли производитель со злым умыслом
- степень оказываемого содействия во время инспекции
- вероятность повторного возникновения той же проблемы
- системный характер несоответствия
- исправление несоответствия с момента предыдущей инспекции
- несоответствие затрагивает целостность данных

ФАРМСТРАТЕГИЯ

Р-ФАРМ
Инновационные технологии здоровья

АНАЛИЗ ИНСПЕКЦИОННОЙ ПРАКТИКИ ПРИМЕНИТЕЛЬНО К КОМПЬЮТЕРИЗИРОВАННЫМ СИСТЕМАМ. КАТЕГОРИЗАЦИЯ НЕСООТВЕТСТВИЙ. ПРИМЕРЫ НЕСООТВЕТСТВИЙ.

Наблюдение

В ходе инспекции осуществлялась проверка входа в систему SAP со стороны сотрудников предприятия.

- Сотрудник склада при входе в систему SAP использовал заранее сохраненный пароль;
- При вводе имени пользователя пароль загрузился автоматически.

Приведет ли такая ситуация к выставлению несоответствия при инспектировании?

- Да, такая ситуация результат прямого нарушения требований GMP
- Нет, такой подход допустим
- Неизвестно, представлено недостаточно данных

Наблюдение № 1:

Какие основные риски могут быть в данной ситуации?

- Потеря целостности данных
- Несанкционированный доступ
- Нарушение плана производства
- Регуляторное несоответствие

Категоризация несоответствия:

- Критическое
- Существенное
- Прочее

Что может снизить критичность несоответствия?

- Пароль при входе в операционную систему
- Ограничение доступа сотрудников в склад
- Политика в отношении целостности данных
- Процедура работы с компьютеризированной системой
- Валидация компьютеризированной системы

Пункт правил GMP

- **Замечание:** Не исключена возможность несанкционированного доступа к компьютеризированной системе SAP. Имеется возможность входа в систему SAP по сохраненному ранее паролю.
- **Категория:** Существенное
- **Пункт правил: 77:** П.12.1 Приложение № 11.

Наблюдение

На участке упаковки записи по упаковке велись с использованием компьютеризированной системы.

- На компьютере на участке упаковке есть возможность изменения даты и времени в системе;
- Для установки даты и времени записей по упаковке программное обеспечение использует системное время;
- Не представлено оценка риска влияния изменения системного времени на программное обеспечение.

Приведет ли такая ситуация к выставлению несоответствия при инспектировании?

- Да, такая ситуация результат прямого нарушения требований GMP
- Нет, такой подход допустим
- Неизвестно, представлено недостаточно данных

Наблюдение № 2:

Какие основные риски могут быть в данной ситуации?

- Случайное изменение параметров работы КС
- Несанкционированный доступ
- Нарушение плана производства
- Регуляторное несоответствие

Категоризация несоответствия:

- Критическое
- Существенное
- Прочее

Что может снизить критичность несоответствия?

- Пароль при входе в операционную систему
- Ограничение доступа сотрудников в склад
- Политика в отношении целостности данных
- Возможность отследить изменение даты и времени с помощью контрольных следов
- Валидация компьютеризированной системы

Пункт правил GMP

- **Замечание:** Не исключена возможность конфигурации системы неконтролируемым способом
- **Категория:** Существенное
- **Пункт правил: 77:** П.10. Приложение № 11.

Наблюдение 3

В лаборатории контроля качества для работы с ВЭЖХ используется программное обеспечение Empower 3.

- Для входа в систему имеется три уровня доступа: оператор, супервайзер, администратор;
- Аналитик отдела контроля качества имеет логин и пароль для входа в систему с уровнем доступа администратор;
- Администратор имеет доступ к копированию, изменению и удалению первичных данных.

Замечание

Не обеспечивается целостность первичных данных результатов испытаний методом ВЭЖХ в программе для работы с хроматографическими данными Empower 3.

Категоризация

Критическое Существенное Несущественное

Пункт правил GMP

Замечание: Не обеспечивается целостность первичных данных результатов испытаний методом ВЭЖХ в программе для работы с хроматографическими данными Empower 3.

- **Категория:** Существенное

Пункт правил: 77: П.7.1 Приложение №11.

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.

Наблюдение 4

В лаборатории контроля качества для расчетов результатов анализа используется программа Excel.

- Не представлены документы по квалификации программного обеспечения;
- Результаты расчета используются для выпуска продукции.

Замечание

Не представлены документы подтверждающие проведение квалификации компьютеризированной системы

Категоризация

Критическое Существенное Несущественное

Пункт правил GMP

Замечание: Не представлены документы подтверждающие проведение квалификации компьютеризированной системы

- **Категория:** Существенное

Пункт правил: 77: Принцип Приложение №11.

Применение компьютеризированной системы должно быть валидировано, информационно-технологическая инфраструктура должна пройти квалификацию.

Наблюдение 5

В ходе инспекции были запрошены документы связанные с использованием «контрольных следов» относительно использующейся ERP-системы.

- Не представлена процедура, в которой приводилось требование к GMP-критичному ПО относительно «контрольных следов»;
- Не представлена система «контрольных следов» для ERP системы.

Замечание

Не проводится регистрация обзора изменений и контрольных следов для валидированной компьютеризированной системы.

Категоризация

Критическое Существенное Несущественное

Пункт правил GMP

Замечание: Не проводится регистрация обзора изменений и контрольных следов для валидированной компьютеризированной системы.

- **Категория:** Существенное

Пункт правил: 77: 9. Приложение №11.

9. На основе оценки рисков следует уделить внимание встраиванию в систему возможности создания записей всех существенных изменений и удалений, связанных с областью действия Правил (система, создающая "контрольные следы"). Причины таких связанных с 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.

Наблюдение 6

П.6. Приложение №11.

Не предусмотрен дополнительный контроль точности ввода данных технологического процесса в систему Х.

При проведении технологического процесса супервайзер, при каждой смене продукта вводит данные технологического процесса в компьютеризированную систему Х без контроля второго человека.

Категоризация Существенное

Наблюдение 7

П.7.2 Приложение №11.

Не предоставлены доказательства сохранения данных из компьютеризированной системы на резервный сервер и возможности восстановления данных и проверки точности резервных копий.

Категоризация Несущественное

Наблюдение 8

П.9 Приложение №11.

Не представлена оценка рисков о необходимости встраивания в компьютеризированную систему ERP возможности создания записей всех существенных изменений и удалений (система создающая «контрольные следы»).

Категоризация Несущественное

Спасибо за внимание.

Подготовлено компанией ФАРМСТРАТЕГИЯ по заказу ЕВРАЗИЙСКОЙ АКАДЕМИИ НАДЛЕЖАЩИХ ПРАКТИК в рамках совместной программы содействия технологическому развитию и повышению качества фармацевтического производства в странах – членах Евразийского экономического сообщества.