**Спецификация на ИФА-спектрофотометр (планшетный анализатор)**

Технические требования

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр | | Требование | Примечание |
| Типы используемых стандартных планшет (по количеству лунок) | | 96- | Допускается использование других планшет |
| Используемые длины волн | | 450 нм, 620 нм, 595 нм, 492 нм. | Допускается более широкий ряд длин волн |
| Светорассеяние | | Не более 0,02% |  |
| Точность установки длины волны, нм | | Не более 1 нм |  |
| Уровень абсорбции, ед. опт. Пл. | | От 0,300 до 3,500 | Допускается более широкий диапазон |
| Линейность, ед. опт. пл. | | от 0,000 до 3,000 ± 2% |  |
| Точность фотометрии | в интервале от 0 до 2 ед. опт. пл. | ± 0,005 ед. опт. пл. или ± 1% |  |
| в интервале от 2 до 3 ед. опт. пл. | ± 2 % |  |
| Повторяемость (коэффициент вариации) | в интервале от 0 до 2 ед. опт. пл. | менее 1 % |  |
| в интервале от 2 до 3 ед. опт. пл. | менее 2% |  |

Требования к программному обеспечению

| **Наименование** | **Описание** |
| --- | --- |
| **Резервное копирование (Backup)** | Процедура резервного копирования и восстановления должны быть определены в соответствии с их графиком. Необходимо регулярное создание резервных копий всех соответствующих данных. Данные резервных копий должны храниться в отдельном и безопасном месте.  Сохранность и точность данных резервных копий должны быть проверены во время или по окончании процесса резервного копирования.  Должен быть определен, протестирован и установлен порядок выполнения резервного копирования, архивирования, извлечения и реконструкции (восстановления) данных в соответствии с риском, имеющим отношение к данным, которые обрабатываются с помощью Системы. |
| **Сохранение данных (Data Retention)** | Данные должны быть защищены как с помощью физических, так и электронных средств от повреждений.  Система должна позволять хранить электронные записи таким образом, чтобы их можно было извлекать безошибочно и сразу на протяжении всего срока хранения записей |
| **Восстановление (Restore)** | Возможность восстановления данных должна проверяться во время валидации и периодически контролироваться. |
| **Возможность инспектирования записей (Record Inspectability)** | Система позволяет создавать точные и полные копии электронных записей в формате удобочитаемых распечаток и стандартных электронных форматов (например, PDF, MS Word, MS Excel, т. д.), пригодных для выполнения контроля, обзора и копирование Регуляторным органом. |
| **Ограниченный доступ (Restricted Access)** | Система должна ограничивать логический доступ предварительно авторизованным пользователям. Для платформы операционной системы необходимо указать несколько уровней доступа пользователей (пользователи системы не должны быть администраторами операционной платформы и, следовательно, им не будет разрешено изменять содержимое файлов/папок/хранящихся баз данных). Пользователи, которые получили доступ к операционной платформе, не должны автоматически получать доступ к Системе.  Пароль должен быть известен только пользователю. |
| **Уникальность кодов (Uniqueness of Codes)** | Система должна поддерживать уникальность каждого комбинированного кода-идентификатора и пароля таким образом, чтобы у двух человек не было одинакового сочетания кода-идентификатора и пароля (система должна предотвращать повторное использование предоставленного идентификатора пользователя).  Каждый пользователь должен быть только единственным пользователем, который знает сочетание кода-идентификатора пароля.  Кроме того, любая учетная запись, не используемая в течение определенного периода, должен быть деактивирована. |
| **Проверка полномочий (Authority Check)** | Система должна ограничивать использование функции согласно предварительно настроенным пользовательским профилям, которые поддерживаются. Любые изменения в ролях должны быть утверждены. Также должна быть возможность прослеживать эти изменения. |
| **Автоматический выход (Automatic Log Off)** | В Системе должен быть механизм автоматического выхода после заранее определенного периода бездействия пользователя или механизм, когда после определенного периода бездействия пользователя требуется введение записи идентификатора пользователя.  У пользователей не должно быть возможности изменять данную функцию. |
| **Безопасность профилей пользователей (User Profiles Security)** | Должна быть внедрена процедура обеспечения безопасности, когда определяются профили пользователей с указанием функций пользователей, которые могут ими использоваться. Любые изменения в профилях пользователей должны утверждаться и прослеживаться. Процедура должна позволять отслеживать и по возможности вести контрольный журнал проблем/изменений и аннулирования разрешения доступа к системе/программе/данным. |
| **Сохранность данных/Обнаружение изменённых записей (Data Integrity / Altered Record Detection)** | Записи система GxP должны быть защищены от изменения/удаления. Если записи можно изменить с помощью инструментов вне Системы, Система должна обнаруживать и отслеживать все действия, выполняемые предварительно уполномоченными операторами с записями (даже на самом высоком уровне доступа, таких как Системный Администратор) |
| **Обнаружение неправильного входа (Invalid Entry Detection)** | Система должна иметь возможность обнаруживать неправильный вход (напр., незаполненные или неправильно заполненные поля, которые должны содержать данные, соответствующие значения, ASCII символы только для числовых полей и неправильные форматы, и др.) |
| **Проверка устройства (Device Check)** | Система должна выполнять проверки устройства (например, периодические), чтобы определять при необходимости достоверность источника ввода данных или операционных команд |
| **Аудиторский след (Audit trail)** | Система должна обеспечивать неопровергаемую регистрацию идентичности операторов, которые вводят или подтверждают данные с помощью Аудиторского следа (журнала аудита - прим.перев.), который должен записывать все действия по созданию, изменению или удалению электронных записей с соответствующими метаданными.  Аудиторский след должен создаваться Системой автоматически без каких-либо действий пользователя.  Аудиторский след должен содержать время и дату относительно действия, выполненного с записью.  Изменение данных должно разрешать чтение исходной информации, т. е. Аудиторский след не должен перезаписывать изменения записи на ранее сохраненные данные.  В случае, если причина изменения или удаления GMP данных должна быть оформлена документально, Система должна заставить пользователя ввести причину.  Система должна позволять создавать точные и полные копии аудиторского следа в стандартном формате (ASCII, PDF).  Аудиторский след должен храниться вместе с соответствующими записями в течение всего срока хранения.  Система должна запрещать всем профилям пользователей на любом уровне (включая Системного Администратора) изменять данные или она должна отслеживать любые изменения с постоянными Электронными журналами (Electronic Logs). |
| **Временная ссылка (Temporal Reference)** | Временная ссылка должна быть одинаковой для всех пользователей, в противном случае Система должна синхронизировать автоматически все рабочие станции. Временная ссылка не может быть изменена пользователем. |

Прочие требования

1. Прибор должен быть внесен в государственный реестр средств измерений.
2. Должна быть выполнена первичная поверка прибора.
3. Возможность получения IQ/OQ в качестве опции от производителя.
4. Пуско-наладочные работы и обучение персонала на месте размещения прибора.