СИСТЕМЫ КОНТРОЛЯ ПАРАМЕТРОВ ЧИСТЫХ ПОМЕЩЕНИЙ И ИХ СООТВЕТСТВИЕ CFR 21, ЧАСТЬ 11

Морган Полен, Lighthouse Worldwide Solution; Барри Хилл, Facility Monitoring System.
Статья предоставлена авторами специально для нашего журнала.
Перевод выполнен Е. С. Хозяшевой (РНЦ «Курчатовский институт»)

Морган Полен (Morgan Polen) является вице-президентом по прикладным исследованиям компании Lighthouse Worldwide Solutions, США, которая специализируется на системах контроля параметров чистых помещений для фармакологической и микроэлектронной промышленности, а также для производства жестких дисков. Доктор Барри Хилл (Barry Hill) – директор компании Facility Monitoring System (FMS) (Великобритания), поставляющей счетчики частиц, системы мониторинга окружающей среды и программное обеспечение для медицинской, фармацевтической и полупроводниковой промышленности.

Введение

Администрация по пищевым продуктам и лекарственным средствам Соединенных Штатов (Food and Drug Administration – FDA) – это правительственное агентство, которое несет ответственность за допуск на рынок новых лекарств и контролирует производство фармацевтических препаратов, которые потребляются в США. Все производимые в США и импортируемые медикаменты подчиняются нормам и правилам FDA. Правила различных государств по сути схожи с нормативными документами FDA, но положение на рынке США таково, что приоритет отдается нормам FDA.

FDA требует, чтобы все медикаменты производились в соответствии с действующей редакцией GMP (Good Manufacturing Practice). Фармацевтические предприятия должны подтверждать соответствие этим нормам на всех стадиях производства вплоть до того, пока лекарство не попадет к конечному потребителю. Частью таких проверок является сбор и хранение информации. Сбор и хранение данных о производстве и продукции имеет столь существенное значение, что неудивительно существование множества правил, включая надлежащее ведение учета.

В последнее десятилетие компьютерные системы стали основным инструментом для сбора данных о технологических процессах на производстве. Поэтому давно ожидалось введение норм, которые регулировали бы задачи электронного ведения учета и передачи записей в FDA в электронной форме. Целью введения таких нормативов FDA было обеспечение достоверности и надежности всей представляемой информации, относящейся к выпуску того или иного продукта.

Эти правила были введены в действие в1997 году и названы «Электронные записи; электронная идентификация» [1]. В сокращенном виде на них часто ссылаются как на CFR (Code of Federal Regulations – Кодекс федеральных правил) 21, часть 11, или – совсем коротко – 21 CFR 11 [4].

В развитие 21 CRF, части 11, было выпущено несколько руководств FDA, однако в августе 2003 года все они были заменены документом «Руководство для производства, часть 11, Электронные записи, электронная идентификация, область действия и применение» [2]. В нем FDA изменило свой подход к области применения и приложениям 21 CFR 11, который отныне основывается на оценке анализа рисков для подтверждения соответствия нормам. Такой подход противоположен основной линии предыдущей редакции правил [3], в которых использование электронных записей допускалось лишь как следствие использования компьютерных систем для упрощения накопления информации и составления отчетов с производства.

Большинство предприятий фармакологической промышленности оборудовано системами автоматического сбора данных для измерения таких параметров среды как концентрация частиц, давление, температура и влажность. Эти системы часто называют системами контроля параметров чистых помещений (Facility Monitoring System – FMS).

Системы контроля параметров чистых помещений

Типичная система контроля параметров (рис. 1) имеет в своем составе компьютер, который контролирует входные сигналы, поступающие от сети датчиков. Информация от этих датчиков поступает с временно́й отметкой, сохраняется в базе данных и отображается на экране. Обычно накапливаемые данные сравниваются с предельно допустимыми уровнями и, если возникает необходимость, сигнал тревоги предупреждает обслуживающий персонал с помощью световой или звуковой сигнализации.

Система контроля параметров чистых помещений должна включать в себя специальные средства формирования отчетов. Обычно отчеты содержат диаграммы, статистические данные и таблицы накопленной информации. Эти отчеты являются главным подтверждением для обоснования качества серийных партий изделий.

Очевидно, что системы контроля параметров подпадают под действие 21 CFR, части 11.

Соответствие 21 CFR часть 11

Ошибочно полагать, что любая компьютерная система удовлетворяет требованиям 21 CFR 11 автоматически, сама по себе. Такое соответствие должно охватывать и квалификацию персонала, и его подготовку, и физическое окружение системы, и меры по

обеспечению безопасности. Между тем все эти факторы не могут находиться под контролем производителей систем контроля параметров чистых помещений. Оценка соответствия лежит на конечных пользователях системы, поскольку именно они в конечном счете ответственны перед FDA или какими-либо другими контролирующими структурами.

Когда производители систем контроля параметров заявляют об их «соответствии 21 CFR, часть 11», они обычно осведомлены о многообразии задач, которые имеются в виду, но скрывают их содержание за короткой формулировкой «Обеспечение необходимыми средствами, позволяющими рассматривать систему контроля параметров как часть общей системы, удовлетворяющей 21 CFR часть 11».

Поскольку лишь конечный пользователь может быть главным судьей при определении соответствия 21 CFR 11, это создает проблемы для поставщиков программного обеспечения. Часто возникают два вопроса – во-первых: «Необходимо ли соответствие требованиям для отдельных подпрограмм?»; во-вторых: «Что такое соответствие?», поскольку многие Интерпретации соответствия противоречивы, а в некоторых случаях и взаимно исключающие. Подход FDA, основанный на анализе рисков, означает, что некоторые из правил могут рассматриваться как необязательные, однако с точки зрения производителей систем контроля параметров, это значит, что необходимо добиться соответствия всем правилам, поскольку любой конечный пользователь может совершенно резонно требовать соответствия любой версии 21 CFR, часть 11. Таким образом, в реальности надо добиваться соответствия всем нормативным требованиям.

Безопасность

Физический доступ

Первым уровнем обеспечения безопасности является физический доступ. Неутешительно, но факт, что именно персонал совершает наибольшее число злоумышленных действий по отношению к компьютерной системе и причастен к воровству информации. Ограничение доступа лимитирует число допущенных к системе лиц, уменьшая тем самым материальную угрозу для системы.

Такое простое решение, как установка компьютера в отдельной комнате или кабинете позволяет избежать недозволенного доступа. Если у вас нет ключа от помещения, вы не имеете физического доступа.

Пользовательский доступ

Для доступа в систему от пользователя требуется подтверждение разрешения доступа, обычно путем ввода имени пользователя и пароля. Альтернатива имени пользователя и пароля заключается в применении биометрических измерений и карт-ключей. 21 CFR 11 не предписывает какой-либо определенный вид контроля; содержится лишь указание, что как минимум допустим один метод биометрического контроля или два вида небиометрического.

Имя пользователя и пароль обычно являются приемлемыми методами идентификации. Они дешевы и просты в использовании, а также при этом не возникает проблем с биометрическими показателями. Так, например, идентификация по отпечаткам пальцев бесполезна, если вы должны работать в перчатках.

Тем не менее, использование имени пользователя и пароля может создать риск несанкционированного доступа в случае, если их кто-то узнает. Их можно обнаружить путем отслеживания записей и показаний приборов, кроме того, имена пользователей и пароли можно узнать путем хакерства (наиболее вероятно проникновение в систему путем подбора паролей «социального» типа: имя жены, кличка кота, регистрационный номер автомобиля...).

Этим двум источникам угрозы можно легко противопоставить метод «устаревания» корпоративного пароля и блокировку терминала, а также включение сигнала тревоги при каком-либо количестве неверных вводов пароля. «Устаревание» пароля вынуждает пользователя через определенный период времени менять пароль на другой, отличный от предыдущих.

Сетевой доступ

Компьютерные системы обычно объединены в сеть, чтобы пользователи могли иметь удаленный доступ к информации. В 21 CFR часть 11 дано определение двух видов систем: открытой и закрытой. Различие между открытой и закрытой системами служит предметом многочисленных дискуссий и, в конечном счете, является вопросом мнений. Закрытая система определяется как система, в которой ее владелец имеет полный контроль над доступом к системе и ее данным.

Открытая система – это та, в которой владелец системы не имеет полного контроля над доступом к системе и ее данным. Примером являются системы, доступ к которым может осуществляться через Интернет. Информация, за исключением зашифрованной, может быть считана третьей стороной и, в принципе, изменена третьим лицом. Но если информация зашифрована, то при соединении через Интернет (обычно) ничего случиться не может.

Можно возразить, что система, в которой используется зашифрованная информация, всегда является закрытой, так как любая информация, собранная третьим лицом, в этом случае бесполезна. Другими словами, введение защиты в открытую систему (чтобы удовлетворить 21 CFR часть 11) часто превращает эту систему в закрытую.

Большинство существующих систем контроля параметров чистых помещений – это закрытые системы. Они отвечают за наблюдение за строго определенными зонами внутри предприятия. Редко может возникнуть необходимость обеспечивать доступ в такую систему откуда-то вне предприятия, поэтому

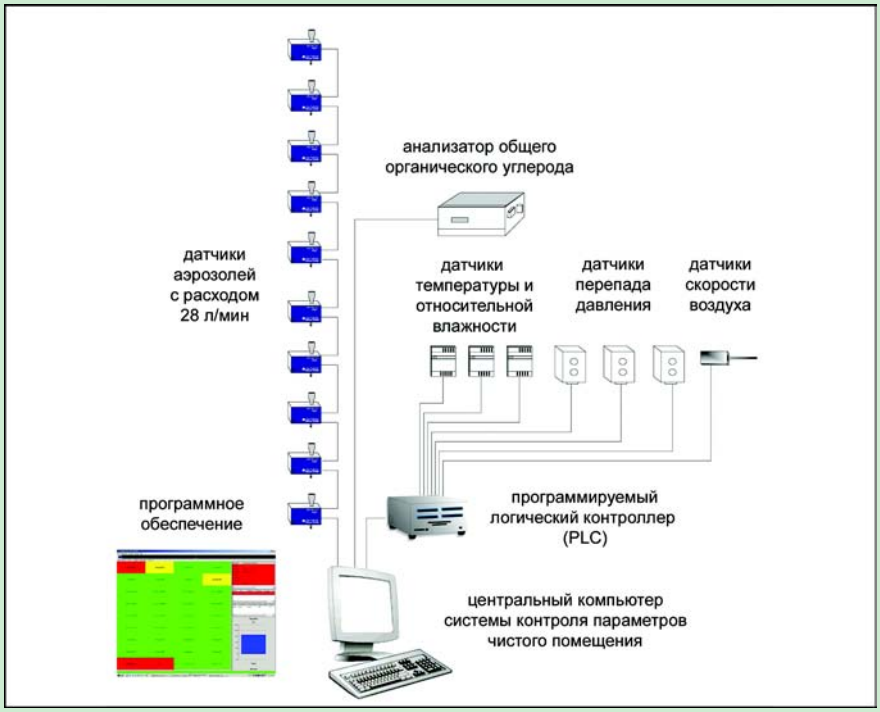

Рис. 1.

систему контроля параметров чистых помещений не имеет смысла делать никакой другой, нежели закрытой.

Система контроля параметров, имеющая выход к общую сеть, должна иметь контроль доступа, который должен осуществляться только через те компьютеры сети, которым это разрешено.

Простые средства контроля доступа по протоколу TCP/IP осуществляются путем использования такой сетевой конфигурации (сетевой маски), которая может значительно ограничить контакты между компьютерами, даже если они физически взаимно связаны.

Широкий доступ можно ограничить путем применения IP-адресов, которые не распознаются через Интернет (они начинаются с цифр 192.168.) и которые не только предотвращают доступ извне предприятия, но также и доступ из той части локальной сети предприятия (Local Area Network – LAN), которая не входит в систему контроля параметров чистого помещения. Промежуточный сервер (прокси-сервер), с одной стороны, может сделать возможным соединение из системы контроля параметров с любой другой системой через Интернет, но, с другой стороны, этот процесс можно контролировать и, при необходимости, предотвращать проникновение извне путем применения аппаратно-программных средств межсетевой защиты (брандмауэр).

Контрольный журнал

В соответствии с 21 CFR 11 при любом режиме работы важно регистрировать доступ пользователей к системе и любые изменения в системе, а также содержание этих изменений.

Контрольный журнал фиксирует производящего действие, причину выполнения действия, а также и саму процедуру действия.

Обычно эти записи должны быть помечены путем использования электронной идентификации (описано ниже). Это связывает определенные действия с соответствующим субъектом. В системе, входящей в сеть, используемый компьютер обязательно должен быть идентифицирован.

Контроль обновлений

При изменении каких-либо параметров системы контроля чистого помещения необходимо иметь возможность даже спустя некоторое временя возвратиться к старой конфигурации. Это можно сделать, если фиксируются содержание и результат проведенных изменений.

Контроль обновлений может представлять из себя систему полного контроля, которая позволит отслеживать и восстанавливать любые сочетания предыдущих версий или, для экономии времени, просто сохранять все варианты конфигураций.

Защита данных

Существует два типа защиты данных, которые противоположны по подходу. Первый вид зашиты данных предполагает хранение информации без доступа к ней, а другой вид защиты заключается в хранении информации с открытым доступом на протяжение большого периода времени.

Если система контроля параметров не относит накопленную информацию к конфиденциальной (примером могут быть истории болезни), то собранная информация с малой вероятностью будет востребована вне организации; поэтому такие данные не представляют из себя секрета. Тем не менее, информация должна быть достоверной, поэтому любое ее изменение должно быть зарегистрировано, а сам факт изменения должен быть отражен в сообщении.

Наипростейшим методом защиты информации является введение циклического контроля с избыточными кодами (Cyclic Redundancy Check – CRC [6]) при каждой записи информации. В этом случае при любой операции с данными проводится сравнение CRC кодов и, таким образом, контролируется сохранность информации. Поскольку учитывается размер и расположение кода, любое незафиксированное изменение данных становится практически нереальным.

Доступ к информации и ее изменение становятся чрезвычайно сложной задачей при использовании шифрования. Зашифровка заключается в разделении данных и перемешивании фрагментов с помощью определенного ключа. Изменение данных при этом затруднено тем, что наблюдатель имеет дело не с понятной упорядоченной информацией, а с беспорядочной последовательностью, полученной особым образом. Например, в [5] представлен простой алгоритм шифрования.

Проблема шифрования состоит в том, что данные можно восстановить только если известен метод дешифровки. Это может создать трудности по прошествии длительных периодов времени.

Например, если пациент проживет 80 лет, то есть вероятность, что необходимо будет изучить воздействие лекарств, которые ему давали в детстве, на его состояние в пожилом возрасте, причем эта информация может потребоваться, например, через 100 лет после того, как данные были записаны. При существующей скорости устареваемости компьютерных систем можно ожидать, что способ дешифровки закодированной информации уже не будет известен тогда, когда информация будет востребована. Шифрование (и аналогичные способы архивирования данных) имеет еще один недостаток, заключающийся в том, что при утере какой-либо части данных теряется весь массив зашифрованной информации.

Одним из путей, обеспечивающих долговременную защиту и хранение информации, является сохранение этой информации в виде открытого незашифрованного текста. Это с наибольшей вероятностью даст возможность прочитать и интерпретировать ее в любой момент на протяжении долгого периода времени. Хотя, конечно, для конфиденциальной информации есть риск быть незаконно скопированной.

В идеале, система контроля параметров чистого помещения должна стараться сохранить информацию путем использования обоих методов, а также обеспечивать широкое использование баз данных, например, SQL серверов.

Электронная идентификация

Об электронной идентификации говорят, что это буквально то же самое, что и индивидуальная подпись человека. Электронная идентификация – это не то же самое, что цифровая подпись.

Цифровая подпись аналогична контрольной сумме, прикрепляемой к файлу или записи данных для указания их источника и подтверждения достоверности файла или пакета данных. Электронной идентификацией должно служить полное имя пользователя. Например, регистрационным именем пользователя может быть «jbloggs», но его электронной идентификацией должно быть «John X. Bloggs».

Для гарантии достоверности любой электронной идентификации необходимо, чтобы администратор системы контроля параметров чистых помещений подтвердил, что регистрационное имя пользователя (user account name) и соответствующая ему электронная идентификация существуют в единственном числе и не могут использоваться повторно. Также важно, чтобы электронная идентификация отличалась от регистрационного имени пользователя, так как она составляет половину данных, необходимых для того, чтобы войти в систему контроля параметров чистого помещения.

ЛИТЕРАТУРА

1. 21 CFR Part 11. Electronic Records; Electronic Signatures; Final Rule Electronic Submissions; Establishments of Public Docket; Notice. 21 CFR 11 Final Rule.
2. Guidance for Industry Part 11, Electronic Records; Electronic Signatures; Scope and Application, Final Guidance – August 2003.
3. Guidance for Industry 21 CFR Part 11; Electronic Records; Electronic Signatures Maintenance of Electronic Records Draft Guidance, July 2002.
4. Очень полезной ссылкой для доступа к документам, связанным с 21 CFR, часть 11 является веб-сайт www.21CFRPart11.com.
5. Tiny Encryption Algorithm. http://www.ftp.cl.cam.ac.uk/frp/papers/djw-rmn/djw-rmn-tea.html .
6. T. Ritter. The Great CRC Mystery, Dr. Dobb's Journal, №112, February 1986.