Стандарт 21 CFR Part 11 и использование электронных подписей и записей в SCADA-пакете PcVue

С.В. Золотарев (Компания ФИОРД)

Рассматривается поддержка требований стандарта 21 CFR Part 11 в SCADA-пакете PcVue компании ARC Informatique (Франция, www.arcinfo.com). Стандарт 21 CFR Part 11 регламентирует использование электронных подписей и ведение электронных записей. Цель этого стандарта – обеспечить регистрацию всех рабочих условий, влияющих на безопасность, эффективность и качество конечных изделий, вместе с подробностями, связанными с подтверждением идентичности оператора и объяснением предпринятых действий. Компания ARC Informatique стала одной из первых в мире среди поставщиков SCADA-пакетов поддерживать требования этого стандарта, что привело к значительному расширению областей использования SCADA-пакета PcVue.

Ключевые слова: SCADA, стандарт 21 CFR Part 11, электронные подписи, электронные записи.

Стандарт 21 CFR Part 11: регулирование использования электронных подписей и ведения электронных записей

Требования Титула 21 Кодекса федеральных правил 21 CFR Part 11 (Part 11 of Title 21 of the Code of Federal Regulations) "ELECTRONIC RECORDS; ELECTRONIC SIGNATURES" (https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm?CFRPart=11) были разработаны Управлением по продуктам питания и лекарственным препаратам США (FDA – United States Food and Drug Administration, http://www.fda.gov/) в 1997 г. для продвижения и регулирования использования электронных подписей, ведения записей и отчетов во всех отраслях бизнеса. Для краткости, будем этот документ называть стандартом 21 CFR Part 11. FDA имеет большое влияние на формирование норм и инструкций во всем мире в различных видах деятельности, часто напрямую не относящихся к тематике продуктов питания и лекарственных препаратов. Важность соответствия стандарту 21 CFR Part 11 вытекает из положений этого стандарта о том, что электронные отчеты на основе электронных записей, которые отвечают его требованиям, могут использоваться вместо бумажных отчетов (если бумажные отчеты не требуются в явном виде). Требования соответствия стандарту 21 CFR Part 11 могут применяться к компьютерным системам (включая аппаратные средства и ПО), средствам управления и сопутствующей документации.

Системы на базе SCADA-пакета PcVue могут быть сконфигурированы таким образом, чтобы удовлетворять требованиям стандарта 21 CFR Part 11. Однако разработчик должен понимать, какие действия допустимы в соответствии с 21 CFR Part 11, а какие нет. Об этом детально поговорим ниже, для чего рассмотрим интерпретацию (реализацию) требований 21 CFR Part 11 в терминах свойств SCADA-пакета PcVue (точнее сказать, ядра PcVue – Супервизора PcVue). Чтобы соблюдать требования стандарта 21 CFR Part 11, все рабочие условия, влияющие на безопасность, эффективность и качество конечных продуктов (изделий), должны регистрироваться вместе с подробностями, связанными с подтверждением идентичности оператора и объяснением предпринятых действий. Эти записи должны храниться в надежном месте и быть готовыми к просмотру как в электронном виде, так и на носителе для чтения человеком. Разработчики PcVue делают одну очень существенную оговорку, что, в конечном счете, гарантирование выполнения требований 21 CFR Part 11 является ответственностью людей или компании, разрабатывающей приложение (то есть системного интегратора). Разработчик должен понимать, что использование заложенных в PcVue возможностей не является гарантией соответствия требованиям 21 CFR Part 11, потому что одно ПО не может обеспечить полного соответствия. Многие из требований должны быть выполнены процедурно, в то время как другие проблемы могут быть решены ограничением доступа к компьютеру и физически, и с помощью электроники. Например, ПК, на котором записываются файлы, должен и физически, и электронным способом обеспечивать предотвращение вмешательства в файлы. Нужно обратить внимание на регулярное архивирование файлов на доступных только для чтения носителях типа CD-R.

Стандарт 21 CFR Part 11 состоит из трех разделов, каждый из которых в свою очередь делится на параграфы, и имеет следующую структуру:

1. Раздел A – Общие условия. Включает следующие параграфы: §11.1 – Область, §11.2 – Реализация, §11.3 – Определения. Раздел А описывает область видимости, исполнение и определения терминов, используемых в 21 CFR Part 11;

2. Раздел B – Электронные записи. Включает параграфы: §11.10 – Средства управления для закрытых систем, §11.30 – Средства управления для открытых систем, §11.50 – Проявления Подписи, §11.70 – Связывание Подписи/Записи. Раздел В описывает требования к средствам управления записями для закрытых и открытых систем;

3. Раздел C – Электронные подписи. Включает параграфы: §11.100 – Общие требования, §11.200 – Электронные компоненты подписи и средства управления, §11.300 – Средства управления для кодов идентификации/паролей. Раздел С описывает исполнение и использование электронных подписей.

Ясное понимание терминологии имеет важное значение для общего понимания стандарта 21 CFR Part 11 и, следовательно, его применения в SCADA-

системах. Поэтому остановимся на некоторых терминах стандарта, применимых к SCADA-системам.

Электронной записью является любая комбинация текста, графики, данных, аудио, изобразительной или другой информации, представленной в цифровой форме, которая создается, модифицируется, сопровождается, архивируется и восстанавливается или распределяется компьютерной системой.

Закрытая система определена как среда, в которой доступом к системе управляют люди, ответственные за содержание электронных записей, находящихся в системе. Как правило, системы управления, построенные на базе SCADA-пакетов, являются закрытыми системами.

Открытая система – среда, в которой доступом к системе не управляют люди, которые ответственны за содержание электронных записей, находящихся в системе. Например, фактически все системы в аналитических лабораториях – закрытые системы. Вместе с соответствующей системой безопасности у лаборатории есть полный контроль над тем, кто получит доступ к системе. Открытая система в лаборатории была бы там, где данные хранятся на сервере, который находится под контролем третьей стороны. Другие примеры для открытых систем – Web-сайты, где у всех есть свободный доступ.

Электронной подписью является компиляция компьютерных данных любого символа или серии символов, оформленных, принятых или санкционированных человеком, чтобы быть юридически обязывающим эквивалентом рукописной подписи человека. Это электронный эквивалент рукописным подписям на бумаге. Они могут быть основаны на методах биометрической идентификации, таких как сканеры отпечатка пальца, вид лица и голосовая идентификация, но возможна достаточна простая комбинация идентификатора пользователя и пароля. В пределах компании идентификатор пользователя должен быть уникальным для определенного человека. Электронные подписи достаточны для закрытых систем.

Цифровая подпись – электронная подпись, основанная на методах шифрования установления подлинности создателя, вычисленного при использовании ряда правил и ряда параметров таким образом, что могут быть проверены личность подписывающего лица и целостность данных. Цифровые подписи требуются для открытых систем и нуждаются в более высоких уровнях безопасности. Поэтому, в дополнение к электронным подписям, должны использоваться методы шифрования для установления подлинности пользователя и целостности записи.

Конфигурирование PcVue в соответствии с требованиями стандарта 21 CFR Part 11

Проанализируем текст стандарта 21 CFR Part 11 и покажем, как те или иные его требования реализованы в PcVue. Для этого тексты параграфов из 21 CFR Part 11 даются курсивом, а их интерпретация (реализация) в PcVue дается обычным шрифтом.

Раздел B стандарта 21 CFR Part 11 (Электронные записи)

§11.10 Средства управления для закрытых систем

Лица, которые используют закрытые системы для создания, изменения, сопровождения или передачи электронных записей, должны использовать процедуры и средства управления, разработанные, чтобы гарантировать подлинность, целостность и при необходимости конфиденциальность электронных записей, и гарантировать, что подписывающее лицо не может аннулировать подписанную запись, как не подлинную. Такие процедуры и средства управления должны включать следующее:

(d) Ограничение доступа к системе для авторизованных лиц.

Супервизор PcVue должен быть сконфигурирован так, чтобы обеспечивать доступ только зарегистрированным пользователям.

(e) Использование безопасных, генерируемых компьютером, аудиторских следов с временными метками, чтобы независимо записывать дату и время входов оператора и действий, которые создают, изменяют или удаляют электронные записи. Изменения записи не должны скрывать предварительно зарегистрированную информацию. Такая документация аудиторского следа должна сохраняться в течение периода, по крайней мере, пока она требуется для подчиненных электронных записей, и должна быть доступна для просмотра и копирования.

Супервизор PcVue может быть сконфигурирован для обеспечения аудиторским следом (журналом) следующих пользовательских действий: вход/выход в/из системы, изменение значения переменной БД, посылка рецепта, подтверждение тревоги, маскирование тревоги, выполнение программы SCADA BASIC. Для разрешения записи предыдущего значения и подписей переменной БД могут быть использованы расширенные атрибуты. Используя расширенные атрибуты переменной, можно записывать дополнительную информацию, когда переменная регистрируется после действия пользователя типа "Загрузка регистра". Расширенные атрибуты позволяют конфигурировать и делать запись для каждой переменной в виде дополнительных 14 текстовых строк, содержащих различную информацию, плюс бинарный образец, характерный для каждой переменной.

Расширенные атрибуты переменной позволяют также регистрировать предыдущее значение регистровой переменной. При регистрации изменения значения регистровой переменной в результате анимации "Загрузка регистра" полезно записывать предыдущее значение регистра наряду с новым (новое значение регистрируется по умолчанию и может быть отображено с использованием мнемоники #C в конфигурации "Окна журнала").

Для записи предыдущего значения регистра используется расширенный атрибут, сконфигурированный для отображения предыдущего контрольного значения. Чтобы сконфигурировать расширенный атрибут для предоставления предыдущего контрольного значения, требует-

ся отредактировать файл конфигурации VARCONF.DAT, добавив строку Set=%PreviousControlValue% после определения атрибута.

Супервизор PcVue не может быть сконфигурирован так, чтобы обеспечить аудиторским следом (журналом) следующие пользовательские действия (поэтому они не должны включаться в систему, совместимую с 21 CFR Part 11): создание, изменение или удаление рецепта, расписания или переменной, проверка правильности пакетной записи, изменение содержания мнемосхем. Указанные действия могут быть запрещены путем использования run time лицензии.

(g) Использование проверок полномочий для гарантирования того, что только авторизованные лица могут использовать систему, делать электронную подпись записи, иметь доступ к функционированию, к входным/выходным устройствам компьютерной системы, изменять запись или выполнять действия вручную.

Супервизор PcVue должен быть сконфигурирован так, чтобы обеспечивать доступ только зарегистрированным пользователям, которые авторизуются путем регистрации с именем и паролем перед доступом к системе.

§11.50 Проявления подписи.

(a) Подписанные электронные записи должны содержать информацию, связанную с подписанием, которое ясно указывает все следующее:

(1) Печатное имя подписывающего лица;

(2) Дату и время, когда подпись была выполнена;

(3) Назначение (например, обзор, одобрение, ответственность или авторство), связанное с подписью.

Система регистрации супервизора PcVue должна быть сконфигурирована так, чтобы имя подписывающего лица (пользователя), время, дата и действие записывались как часть любой записи.

Раздел С стандарта 21 CFR Part 11 (Электронные подписи)

Интерпретация электронной подписи для супервизора PcVue – это комбинация имени пользователя и пароля, плюс другая необязательная информация типа имени и фамилии, вместе известная как учетная запись пользователя. Чтобы разрешить некоторые из особенностей, необходимых для 21 CFR Part 11, в диалоговом окне "Общее функционирование" должно быть отмечено свойство "Разрешить иерархические профили пользователей". Для гарантирования целостности конфигурационного файла прав пользователя должна быть выбрана опция для его шифрования.

§11.100 Общие требования

(a) Каждая электронная подпись должна быть уникальной для одного индивидуума и не должна многократно использоваться или переназначаться кому-либо еще.

Имена, используемые во всех учетных записях PcVue, должны быть уникальными. Если Учетная запись пользователя удаляется, ее информация сохраняется, так что имя не может многократно использоваться.

Все пароли, используемые в проекте PcVue, включая любые истекшие или используемые в удаленных учетных записях, должны быть уникальными. Чтобы гарантировать это, внутренняя запись сохраняет до 1000 предыдущих паролей. Пароли должны содержать 6 или более символов. В PcVue введана специальная встроенная оценки "прочности" пароля при добавлении в систему пользователя по шкале слабый-средний-строгий.

§11.200 Компоненты и средства управления электронными подписями

(a) Электронные подписи, которые не основаны на биометрии, должны:

(1) Использовать, по крайней мере, два отличных идентифицирующих компонента.

Учетная запись пользователя включает, по крайней мере, имя пользователя и пароль.

(i) Когда индивидуум выполняет серию подписаний в течение отдельного, непрерывного периода доступа к контролируемой системе, первое подписание должно быть выполнено с использованием всех электронных компонентов подписи; последующие подписания должны быть выполнены с использованием, по крайней мере, одного электронного компонента подписи, который является исполняемым и предназначенным только к использованию индивидуумом.

Когда пользователь регистрируется в системе (первое подписание), должны быть введены как имя пользователя, так и его пароль, что является нормальным для супервизора PcVue. Для последующих подписаний, например, с использованием зоны управления для изменения значения переменной, пользователь должен заново ввести, как минимум, пароль. Для достижения этого в любой зоне управления должна быть использована анимация "Безопасность", которая предполагает требование электронной подписи.

(ii) Когда индивидуум выполняет одно или более подписаний, не обеспечиваемых в течение отдельного, непрерывного периода доступа к управляемой системе, каждое подписание должно быть выполнено с использованием всех электронных компонентов подписи.

При использовании анимации "Безопасность" для безопасности зоны управления она не может быть активизирована, пока пользователь не зарегистрируется.

(2) Быть использованными только их подлинными владельцами.

Когда администратор создает учетную запись пользователя, ей задаются имя и пароль. Когда учетная запись используется в первый раз, пользователь должен изменить пароль так, чтобы это было известно только ему. Как только учетная запись была создана, она может быть только дезактивирована (в таком случае она может быть реактивирована) или удалена администратором. Информация удаленных учетных записей сохраняется. Удаленная учетная запись не может быть обновлена.

(3) Требовать участия двух или более лиц при управлении и выполнении, чтобы гарантировать, что предпринятое использование электронной подписи проводится ее подлинным владельцем.

Для удовлетворения этого требования в PcVue используется анимация "Безопасность" (рис.1), которая предоставляет разработчику очень широкие возможности. Использование этой анимации в сочетании с командной зоной позволяет требовать от оператора:

• повторно ввести пароль, прежде чем получить доступ к элементу;

• ввести дополнительный идентификатор и дополнительный пароль, прежде чем получить доступ к элементу. Это позволяет удовлетворить требование 21 CFR Part 11 участия двух или более лиц при управлении и выполнении и требовать (как минимум) двойной подписи;

• повторно ввести пароль, а также дополнительный идентификатор и дополнительный пароль, прежде чем получить доступ к элементу.

(b) Электронные подписи, основанные на биометрии, должны разрабатываться с гарантированием того, что они не могут быть использованными кем-то другим, кроме их подлинных владельцев.

Данное требование стандарта 21 CFR Part 11 не поддерживается средствами конфигурирования супервизора PcVue.

§11.300 Средства управления для идентификации кодов/паролей.

Лица, которые используют электронные подписи, основанные на использовании идентифицирующих кодов в комбинации с паролями, должны использовать средства управления для гарантирования их безопасности и целостности. Такие средства управления должны включать:

(a) Сопровождение уникальности каждого объединенного идентифицирующего кода и пароля так, чтобы никакие два человека не имели одинаковую комбинацию идентифицирующего кода и пароля.

Имена, используемые во всех учетных записях, должны быть уникальными. Если учетная запись пользователя удаляется, ее информация сохраняется, так что имя не может многократно использоваться.

Пароли, используемые во всех текущих учетных записях пользователя, должны быть уникальными. Запись сохраняет до 1000 предыдущих паролей, обеспечивая (в пределах разумной вероятности), что все пароли уникальны. Пароли должны содержать 6 или более символов.

(b) Гарантирование того, что идентифицирующий код и пароли периодически проверяются, заново вызываются или пересматриваются (например, чтобы учесть такие события как истечение срока действия пароля).

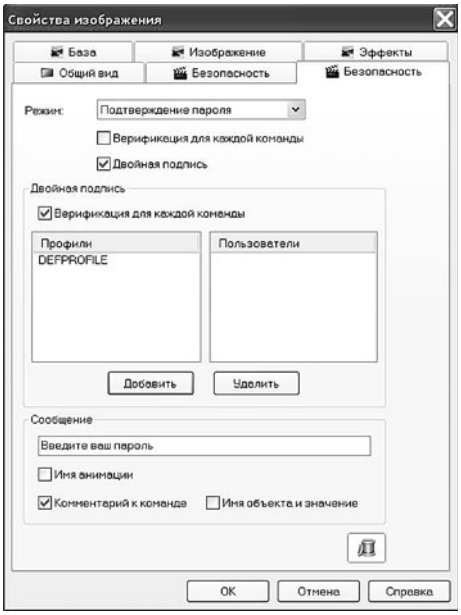

Рис. 1. Анимация "Безопасность"

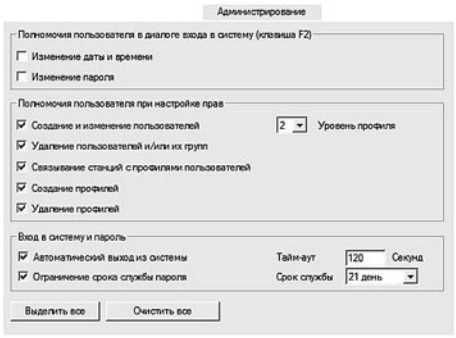

Рис. 2. Пример ограничения срока службы пароля в PcVue

Свойство "Ограничение срока службы пароля" в закладке "Администрирование профиля пользователя" используется, чтобы пользователь был вынужден периодически изменять пароль (рис. 2) .

(c) Следование процедурам контроля потери управления, чтобы электронным способом запретить использовать потерянные, украденные, отсутствующие или иначе потенциально представляющие угрозу указатели, платы и другие устройства, которые имеют или генерируют идентифицирующий код или информацию пароля, и выпускать временные или постоянные замены, использующие подходящие строгие средства управления.

Учетные записи могут быть дезактивированы или удалены. Дезактивированная учетная запись может быть повторно активирована. Удаленная учетная запись не может быть обновлена.

(d) Использование мер безопасности транзакции, чтобы предотвратить неправомочное использование паролей и/или идентифицирующих кодов, и обнаруживать и сообщать немедленно и самым срочным способом о любых попытках их неправомочного использования системному модулю безопасности и организационному управлению.

Каждый раз, когда происходит неудавшийся вход в систему, генерируется тревога, использующая переменную SYSTEM. <StationName>. USER.REJECTED. После трех неудавшихся попыток входа в систему учетная запись дезактивируется.

PcVue и обеспечение аудиторского следа

Для обеспечения аудиторского следа пользовательских действий в PcVue используются:

• фильтры журнала выбирают регистрируемые действия и место их сохранения;

• архивные модули сохраняют зарегистрированные действия;

• окно журнала предоставляет способ рассмотрения зарегистрированных действий, которые были сохранены в архивных модулях.

В документации на PcVue детально описано, как конфигурировать фильтры журналов, архивные модули и окна журнала. Зарегистрированные записи,

Таблица

Источник и Действие	Опция в конфигурации фильтра журнала
Анимация – Загрузка бита	Команда
Анимация – Загрузка регистра	Команда
Анимация – Загрузка текста	Команда
Анимация – Рецепт	Команда
Анимация – Выполнение программы	Программа
Окно тревоги – Подтверждение тревог	Подтверждение
Окно тревоги – Маскирование тревоги	Действие маски
Регистрация	Регистрация/Выход

использующие фильтры журнала не зашифрованы. Поэтому необходимо обеспечить некоторые другие средства защиты их от вмешательства, наподобие ограничения физического доступа на компьютер, на котором они размещаются.

В PcVue могут быть зарегистрированы следующие пользовательские действия в режиме выполнения (таблица).

Если выбрана опция "Регистрация/Выход", неуспешные входы в систему также регистрируются. Автоматический выход их системы из-за периода бездеятельности записывается как нормальный выход их системы.

Следующие действия пользователя во время выполнения не могут быть зарегистрированы, и поэтому их использование нужно тщательно рассмотреть в проекте, совместимом с 21CFR Part 11: изменение системной даты и времени в диалоге входа, анимации "Загрузить расписание", "Открытие связи", "Закрытие связи", "Гиперссылка", "Примечание", "Запуск макроса", "Выполнение приложения", "Создание, изменение или удаление рецепта" или расписания.

В PcVue нет возможности записать индивидуальные изменения, сделанные в конфигурации проекта, когда он находится в режиме конструирования. Поэтому предполагается, что однажды принятый проект, совместимый с 21 CFR Part 11, используется только с ключом защиты run time (то есть в режиме выполнения).

Заключение

В настоящее время соблюдение требований стандарта 21 CFR Part 11 считается важным не только в SCADA-пакетах, но и в других компьютерных системах, таких как EDMS (системы управления документами), ERP (системы планирования ресурсов предприятия), MRP (системы планирования потребностей в материалах), WMS (системы автоматизации склада), LIMS (лабораторные информационно-управляющие системы), ПЛК (http://www.labcompliance.com/tutorial/part11/default.aspx). Даже офисные программные продукты обращают пристальное внимание на требования стандарта 21 CFR Part 11, например, Microsoft Office 2007 (http://www.microsoft.com/office/showcase/2007/cfr/partnersol.mspx).

Необходимость соответствовать требованиям стандарта 21 CFR Part 11 в SCADA-системах заставило многих разработчиков таких систем внести серьезные доработки в свои продукты, касающиеся использования электронных подписей и ведения электронных записей. Одной из первых в мире это сделала французская компания ARC Informatique в своем популярном SCADA-пакете PcVue, что значительно повысило конкурентные преимущества PcVue.

Золотарев Сергей Викторович *– канд. техн. наук, ведущий эксперт компании ФИОРД.*

Контактный телефон (812) 323-62-12.

E-mail: zolotarev@fiord.com