Обеспечение информационной безопасности при применении SCADA-системы SIMATIC WinCC Open Architecture

А.С. Мельников, С.Ю. Соловьев (ООО «Сименс»)

Рассматриваются подходы к обеспечению информационной безопасности при применении SCADA-системы SIMATIC WinCC OA Open Architecture с учетом организационной и технической составляющих.

Ключевые слова: SCADA-система, информационная безопасность, организационные и технические мероприятия, ячейки безопасности.

Введение

Задача повышения эффективности, стоящая перед любым современным бизнесом, который связан с технологическими процессами, подразумевает применение SCADA-систем, позволяющих создавать масштабируемые распределенные высоконадежные решения для диспетчерского контроля и управления.

Рассмотрим подходы к обеспечению информационной безопасности при применении SCADA-системы SIMATIC WinCC Open Architecture (WinCC OA) [1, 2] на примере установки, имеющей архитектуру, представленную на рис. 1.

Организационные аспекты

Начнем с рассмотрения некоторых ключевых организационных аспектов [3], без которых применение технических мер защиты не только неэффективно, но зачастую и невозможно.

С целью обеспечения системного подхода в отношении информационной безопасности (ИБ), включая кибербезопасность, в организации должна быть официально инициирована программа обеспечения защищенности систем управления и промышленной автоматики (например, согласно стандартам IEC 62443, ISO27xxx).

При этом в связи с прямой зависимостью между инцидентами и финансовыми, репутационными и прочими потерями лучшей практикой считается курирование вопросов ИБ на уровне высшего руководства компании.

К сожалению, в связи с тем, что ИБ является бизнес-процессом в основном с фоновыми «непонятными» активностями, данная область часто рассматривается как второстепенная, а финансирование осуществляется по остаточному принципу.

Для формирования должного внимания к данной области может быть внедрен процесс учета и регистрации финансовых потерь, связанных с инцидентами, приведшими к снижению доступности и/или потере целостности и конфиденциальности, с последующим представлением собранной статистики высшему руководству. Данный процесс целесообразно синхронизировать с процессом DSS02 «Управление запросами на обслуживание и инцидентами» (нумерация согласно COBIT5, www.isaca.org). Дополнительно может быть использован подход, представленный в п. 4.2.2 ГОСТ Р МЭК 62443-2-1-2015 (подготовка «Экономического обоснования» (при наличии явных рисков — без финансовых выкладок) с описанием основных уязвимостей, угроз и возможных последствий).

Не менее важную роль в обеспечении ИБ играет наличие актуальной информации о защищаемой области (места расположения объектов, границы периметров, схемы сетей, перечень и места установки оборудования, версии ПО, места хранения резервных копий и т. п.). Данный аспект представляет со-

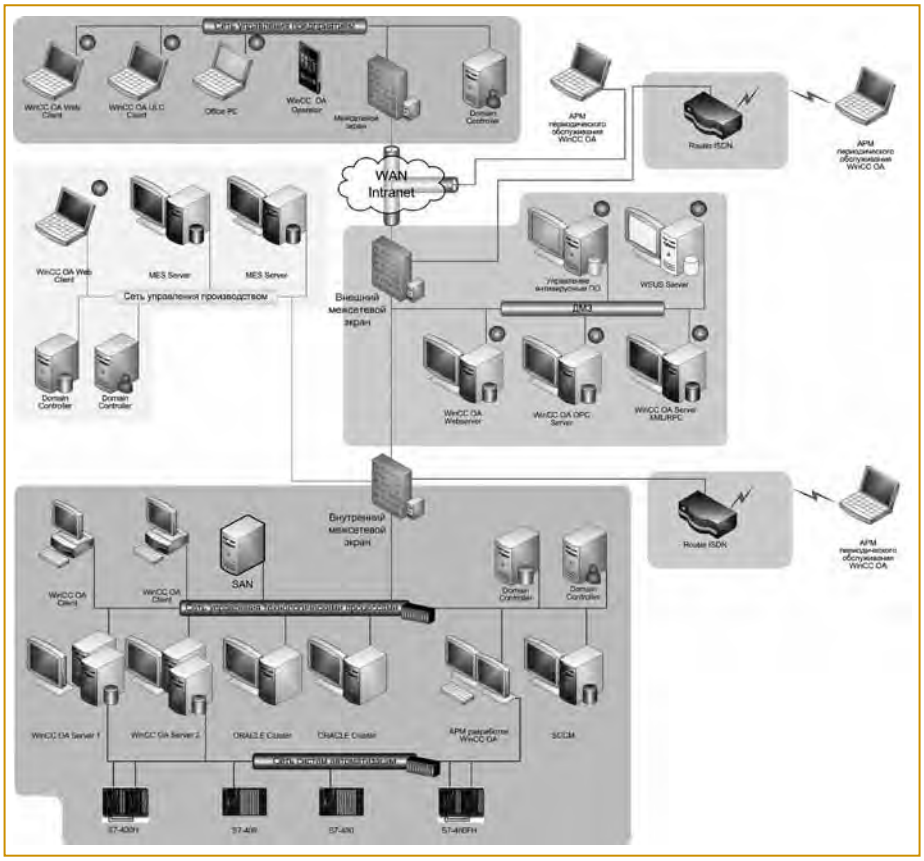

Рис. 1. Пример архитектуры производственной сети

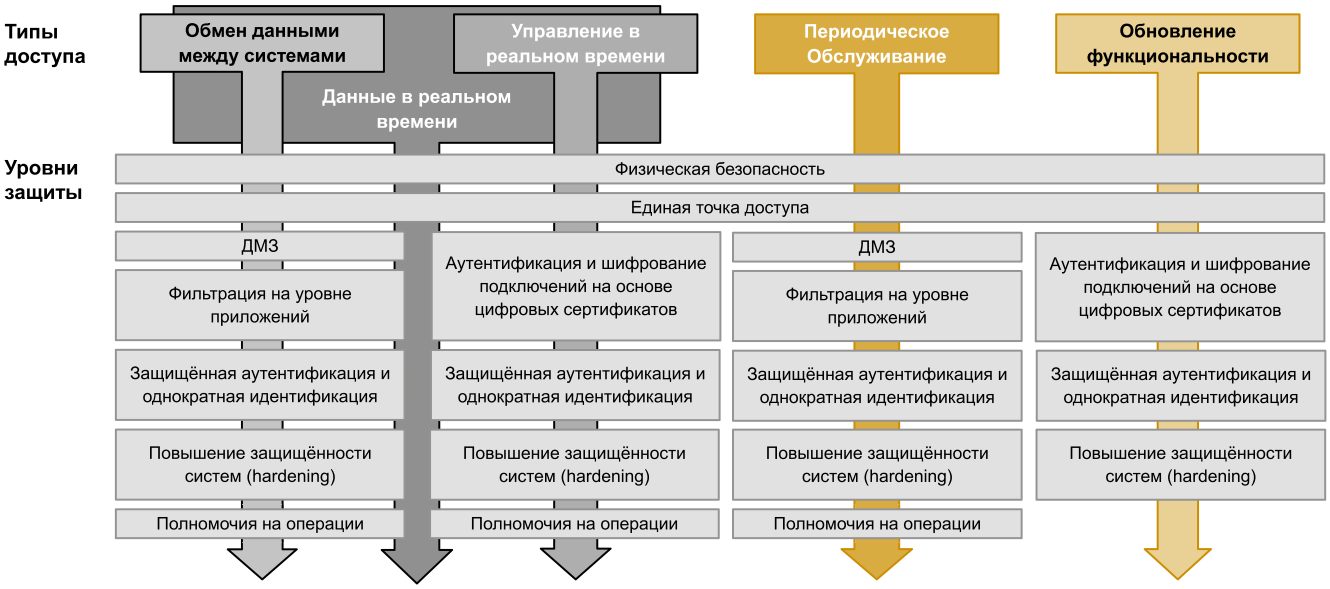

Рис. 2. Типы доступа

бой один из краеугольных камней успеха программы информационной (кибер)безопасности, который в конечном итоге выражается в снижении числа инцидентов и связанных с ними потерь предприятия (финансовых, репутационных и т. п.).

Так, приведенная на рис. 1 схема сети позволяет быстро получить представление об имеющихся производственных объектах и их взаимосвязях. Схема может быть дополнена информацией, например, об используемом оборудовании, версиях ПО, сетевых адресах, коммуникационных маршрутах и др. Профессиональным решением для документирования инфраструктуры предприятия является использование специализированной системы, выполняющей, в том числе и функции полноценной базы данных управления конфигурациями (Configuration management database, CMDB).

Для актуализации информации об имеющихся имущественных объектах используются процессы BAI10 «Управление конфигурациями» и BAI06 «Управление изменениями» (согласно COBIT5). Их реализация в организации не только желательна, но и необходима для эффективного обеспечения безопасности.

Более детально программа обеспечения защищенности (кибербезопасности) систем управления и промышленной автоматики представлена в международных и российских стандартах, например, IEC62443 (ГОСТ Р 56205-2014, ГОСТ Р МЭК 62443 2-1-2015) и т. д. (в связи с особенностями перевода рекомендуется верифицировать русскоязычную версию на предмет соответствия иностранной редакции данных стандартов).

Принципы и подходы к обеспечению ИБ в SCADA-системе WinCC OA

Для обеспечения эффективной защиты при использовании SCADA-систем на базе WinCC OA (и установок в целом) целесообразно применение следующих принципов:

- концепции эшелонированной защиты;
- сегментации на ячейки безопасности;
- предоставления прав и полномочий согласно выполняемым задачам;
- группировки на основе выполняемых задач, централизованного и локального администрирования;
- использования встроенных механизмов обеспечения безопасности SCADA-системы WinCC OA.

Концепция эшелонированной защиты. В рассматриваемом примере предполагается информационное взаимодействие между объектами, находящимися на различных уровнях системы управления, а также за периметром организации.

При этом могут быть определены следующие типы доступа (рис. 2):

- обмен данными между системами — обмен данными между различными уровнями производства, смежными системами, удаленными и локальными компонентами, ячейками автоматизации и безопасности;
- управление в режиме реального времени/удаленное управление — мониторинг и управление установкой с полевого уровня или из удаленного центра управления;
- периодическое обслуживание — регулярный мониторинг системы и архивирование диагностической информации, резервное копирование данных, установка программных обновлений (updates) или тонкая настройка системы;
- обновление функциональности — все активности, связанные с инжинирингом, модернизацией (upgrade) или изменениями в системе управления процессами, в том числе исправление ошибок;
- данные в реальном времени — комбинация типов "обмен данными" и "управление в режиме реального времени": использование подобного комбинированного типа доступа может быть продиктовано сочетанием выполняемых задач. Однако желательно избегать подобного комбинированного типа доступа,

поскольку меры по обеспечению безопасности слишком различны, а компромиссные решения связаны с повышенным уровнем риска.

Риски, связанные с несанкционированным доступом, отличаются для различных типов доступа. Соответственно отдельные подключения, их типы и механизмы осуществления доступа должны быть детально перечислены и классифицированы для последующего анализа и защиты. Особое внимание необходимо уделять безопасности удаленных соединений.

При реализации концепции эшелонированной защиты могут использоваться следующие механизмы обеспечения безопасности:

- физическая безопасность;
- единая точка доступа к каждой ячейке безопасности (на базе межсетевого экрана) для аутентифицированных пользователей, устройств и приложений, обеспечивающая контроль доступа и обнаружение атак. Она служит основной точкой доступа к сети ячейки безопасности и является первым элементом в цепочке контроля прав доступа на сетевом уровне;
- демилитаризованные зоны;
- фильтрация на уровне приложений должна применяться в качестве стандартного решения, то есть каждая отдельная команда может быть проверена на корректность. Данный механизм защиты должен применяться с учетом того, что неисправность подобного механизма не должна влиять на управление процессом. Сканирование входящих данных на предмет наличия вирусов означает, что все файлы и данные, доступные для чтения, принимаемые всеми системами, сканируются на уровне первой системы, разрешающей доступ и позволяющей чтение файлов/данных;
- аутентификация на основе цифровых сертификатов шифрования и шифрование связи;
- однократная идентификация (Single Sign On);
- полномочия на операции. Данный подход является "последней линией обороны" и также именуется "управлением правами доступа".

Сегментация на ячейки безопасности. Стратегия сегментации систем и смежных систем на ячейки безопасности позволяет повысить надежность системы в целом за счет ограничения областей влияния отдельных отказов или угроз, которые могут привести к отказам. Эффективное применение данного подхода подразумевает тщательное предварительное планирование ячеек безопасности. В этой связи система сначала сегментируется на ячейки автоматизации (отдельные элементы технологического процесса), а затем на ячейки безопасности путем применения механизмов безопасности.

Все приведенные в примере на рис. 1 сети, включая находящееся в них оборудование, представляют собой отдельные ячейки безопасности, которые могут работать автономно в течение определенного отрезка времени (рис. 3).

В результате функционирование отдельных ячеек безопасности или сегментов обеспечивается даже в случае временной потери части инфраструктуры. Для этой цели информация и сервисы, которые необходимы для функционирования ячейки безопасности и которые предоставляются извне, должны быть промежуточно сохранены или дублированы внутри ячейки безопасности (например, основные данные материалов, сетевые сервисы — разрешение сетевых имен, выделение IP-адресов и аутентификация пользователей). Соответствующие меры должны быть приняты в рамках ячейки безопасности.

Также внутри ячеек должны быть приняты меры, защищающие данные ячейки от угроз, возникающих в других ячейках безопасности (например вируса, отмеченного коричневым на рис. 4). Таким образом, пока осуществляется устранение информационной угрозы, обеспечивается функционирование всей системы в целом.

Планирование ячеек безопасности должно учитывать текущие зоны ответственности должностных лиц, возможность выделения элементов процессов, вопросы физического доступа, дизайн сети и имеющиеся механизмы контроля доступа.

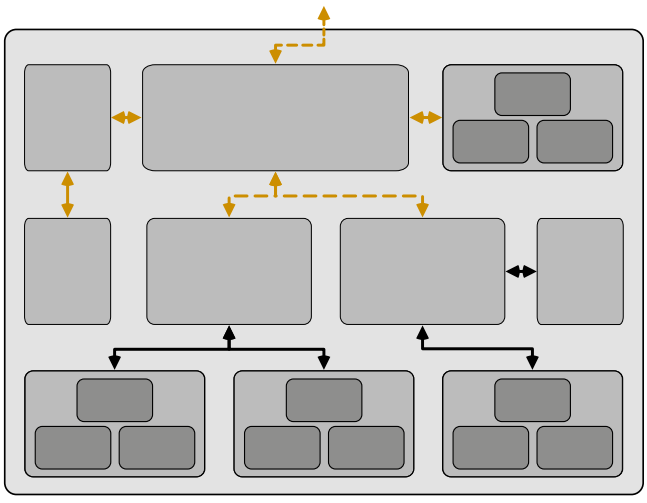

Рис. 3. Обеспечение автономности отдельных ячеек безопасности для случаев временной потери части инфраструктуры (например, сетей, отмеченных коричневым)

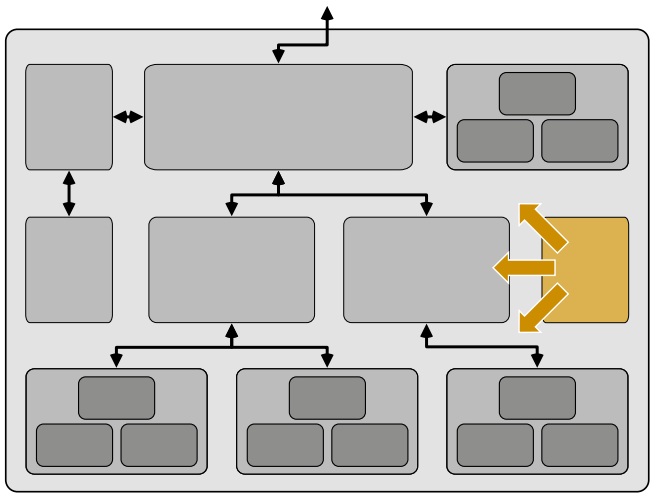

Рис. 4. Защита ячеек безопасности от возможных угроз в других ячейках безопасности

Предоставление прав и полномочий согласно выполняемым задачам. Стратегия предоставления прав и полномочий согласно выполняемым задачам включает ограничение прав пользователей, операторов, устройств, сетей и программных компонентов до необходимого минимума.

Права доступа и полномочия на операции, ориентированные на выполняемые задачи, зависят от ролей. Роли зависят от компетенций и областей ответственности соответствующих операторов установки. Использование подобного подхода позволяет структурировать процесс управления и обеспечить его защищенность даже при его территориальной распределенности и наличии сетей различных типов.

Группировка на основе выполняемых задач, централизованное и локальное администрирование. Группировка систем с одинаковым назначением и с одинаковыми настройками сокращает число ошибок по сравнению с независимым локальным выполнением настроек.

Важные части систем должны быть идентифицированы и сгруппированы таким образом, чтобы администрирование данных групп могло производиться независимо друг от друга. Должна быть обеспечена возможность полного отключения системы управления. Может использоваться, например, следующая группировка:

- серверов WinCC OA согласно их назначению;
- всех UI-клиентов WinCC OA в одной "клиентской группе".

Для всех задач каждой обслуживаемой системы должны быть определены маршруты выполнения данных задач (то есть сетевые маршруты, временная корректировка настроек межсетевых экранов и т. д.).

Все задачи администрирования должны выполняться централизованно (например, путем применения сервера резервного копирования, сервера для проведения централизованных обновлений и т. д.).

При этом для задач администрирования должны быть определены и внедрены соответствующие процессы. Например, можно сформулировать следующие задачи по администрированию, требующие определения и внедрения соответствующих процессов:

— обновление ПО: должен быть определен (разработан) и внедрен процесс планирования и проведения централизованных обновлений ПО, (например, обновлений для системы безопасности, программных исправлений, обновлений вирусных сигнатур, обновлений проектов, установки сертификатов), распространяемых из единой точки;

— настройка ПО: должен быть определен (разработан) и внедрен процесс планирования и выполнения из единой точки централизованных настроек систем (ОС, антивирусной защиты, служб обновлений ОС Windows и т. д.);

— резервное копирование и восстановление данных: должен быть определен и внедрен (разработан) процесс планирования и выполнения резервного копирования и восстановления данных, программ, ОС. Данный процесс должен быть построен с использованием единой системы резервного копирования;

— журналирование и диагностика: должен быть определен (разработан) и внедрен процесс журналирования локальных событий и сохранения соответствующих диагностических журналов, журналов безопасности и прочих журналов в централизованном хранилище.

Любые исключения должны быть обсуждены и скоординированы с оператором системы. Примером подобного исключения может являться создание резервных копий на локальной системе, при котором в случае потери локального хранилища также будут утеряны резервные копии.

Использование встроенных механизмов обеспечения безопасности WinCC OA

С целью реализации перечисленных принципов SCADA-система WinCC OA обладает следующими встроенными механизмами или поддерживает следующие архитектурные решения обеспечения безопасности.

- *Резервирование серверов*. Система WinCC OA поддерживает режим горячего резервирования серверов. При этом оба сервера одновременно принимают информацию с периферийных устройств, но только один из них является активным и формирует команды управления и информационный поток в направлении рабочих станций операторов. Встроенные механизмы синхронизации обеспечивают идентичность образов процесса в обоих серверах. Механизм взаимной проверки состояния серверов обеспечивает передачу управляющей роли между серверами в случае выхода из строя или частичной неработоспособности одного из них. Для повышения надежности решения, для коммуникации серверов между собой и с другими удаленными системами в WinCC OA могут использоваться резервированные каналы связи. При этом речь идет не о механизме, например NIC Teaming, а о параллельной отправке и приеме пакетов через независимые сети. В случае крупных территориально распределенных систем могут использоваться сети различных операторов связи.
- *Резервирование 2x2*. При создании резервных центров управления может быть использована функциональность резервирования 2x2 системы WinCC OA (рис. 5). При этом одна пара серверов в горячем резерве физически находится в одном центре управления, а другая пара серверов также в горячем резерве находится в территориально удаленном резервном центре управления. Активный центр управления взаимодействует с периферией и с рабочими станциями операторов. Встроенные механизмы синхронизации обеспечивают идентичность образов процесса в обоих центрах управления. При ограниченных полосах пропускания в первую очередь синхронизируются значе-

ния полевых сигналов. Механизм взаимной проверки состояния центров управления обеспечивает передачу управляющей роли между центрами управления в случае полного выхода из строя одного из них (то есть выхода из строя обоих серверов основного центра управления). Переключение может быть также инициировано вручную. Коммуникация резервных центров между собой возможна также по резервированным каналам связи.

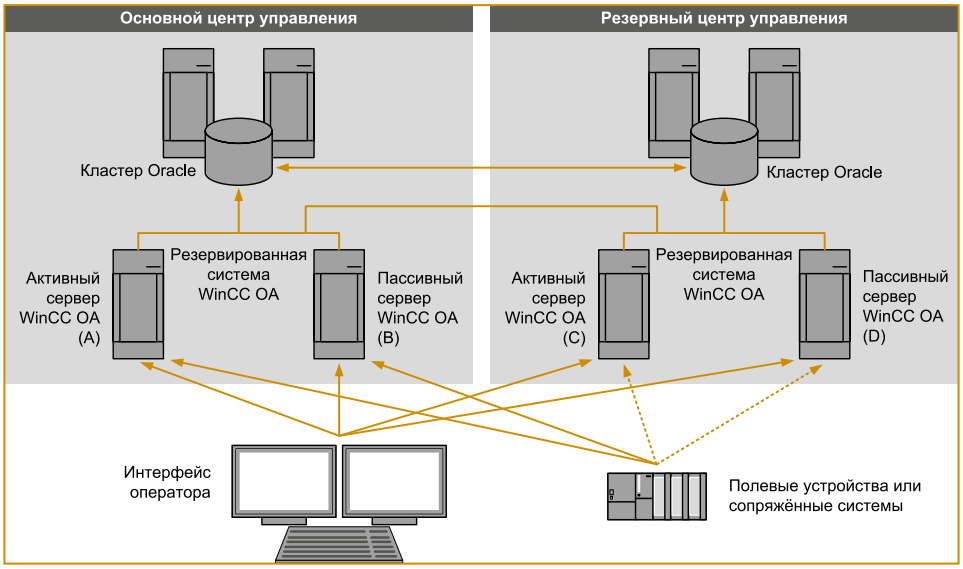

Рис. 5. Архитектура резервирования 2x2

• *Шифрование сценариев и панелей.* Отличительной особенностью WinCC OA с точки зрения обеспечения защищенности систем является наличие функции шифрования файлов проекта (сценариев, панелей). Шифрование панелей препятствует получению злоумышленником информации о внутренних технических деталях проекта. Шифрование не оказывает какого-либо влияния на проект в режиме выполнения.

• *Смена пользователя без закрытия экранной формы процесса.* Система WinCC OA поддерживает смену пользователей без закрытия экранной формы процесса. После выхода пользователя из системы на уровне WinCC OA и до последующей регистрации в системе другого пользователя с достаточным уровнем полномочий никакие действия с экранной формой процесса невозможны. С целью ограничения доступа к рабочему столу ОС может быть использован полноэкранный режим приложения WinCC OA с отключенным заголовком окна (title bar), а также деактивированы стандартные комбинации клавиш, например, <CTRL><ALT><DEL>, клавиша Win и т. п.

• *Аутентификация пользователей* в системе осуществляется на основании имени пользователя системы WinCC OA и пароля. Возможно использование доменных учетных записей Active Directory. Выход пользователя из системы выполняется на уровне ПО системы управления процессами и обычно не сопровождается закрытием экранной формы процесса.

• *Управление полномочиями пользователей* осуществляется путем включения пользователей в одну или несколько групп с дальнейшим присвоением полномочий данным группам на допустимые операции в системе, например, визуализация, базовые операции, администратор, квитирование и т. п.

Возможна синхронизация пользователей и их членства в группах с пользователями и группами в домене Active Directory (полномочия на уровне WinCC OA настраиваются независимо от полномочий в Active Directory).

• *Полномочия для рабочих станций в WinCC OA.* Дополнительно к уровням полномочий отдельных пользователей для рабочих станций WinCC OA могут быть установлены различные уровни полномочий. Подобным образом может быть ограничен набор рабочих станций, с которых выполняется, например, администрирование системы.

• *Полномочия для участков в WinCC OA. В проектах WinCC OA* имеется возможность определения отдельных "участков" (территориальных или организационных областей). Они могут быть использованы для ограничения полномочий пользователей в рамках данных участков.

• *Однократная идентификация (Single Sign On)* позволяет организовать автоматический вход пользователя в WinCC OA с правами учетной записи, имя которой совпадает с именем учетной записи для входа в домен Windows. При этом исключается возможность совершения оператором каких-либо действий на уровне ОС, так как запуск клиента WinCC OA и регистрация в системе WinCC OA осуществляется автоматически непосредственно после входа в домен ОС Windows.

• *Автоматический выход из системы.* Для предотвращения несанкционированных действий со стороны неуполномоченных лиц при отсутствии оператора на рабочем месте может быть использована функция реакции WinCC OA на неактивность пользователя (рис. 6).

Данная функция позволяет определить поведение системы после указанного периода неактивности пользователя. При этом имеется возможность выполнения следующих действий:

– автоматический выход пользователя из системы WinCC OA;

– запуск хранителя экрана;

– выход пользователя из системы WinCC OA и запуск хранителя экрана;

– закрытие подключения локального интерфейса пользователя;

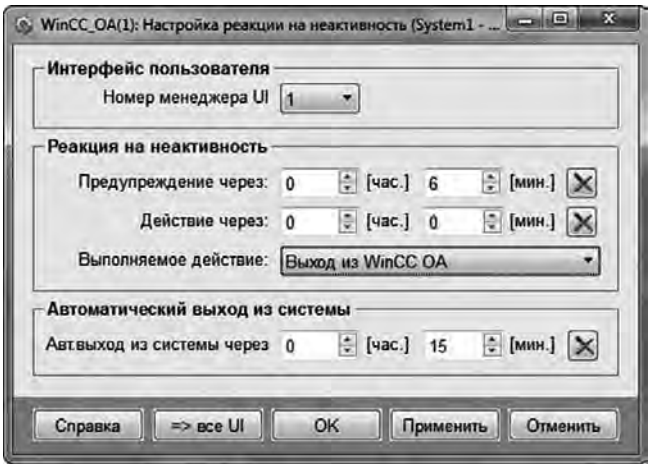

Рис. 6. Панель настройки реакции на неактивность

– выход пользователя из ОС Windows.

• *Журнал использования системы*. Система WinCC OA содержит встроенную систему отчетности обо всех выполненных входах в систему и выходах из системы. В отчете также отображаются номера соответствующих интерфейсов пользователя (номера менеджеров).

• *Журнал действий оператора системы*. Стандартные функции языка программирования Control системы WinCC OA позволяют обеспечить регистрацию действий оператора в системе в отношении объектов управляемой установки.

• *Использование антивирусного ПО*. Система WinCC OA протестирована на совместимость со следующим антивирусным ПО: McAfee Endpoint Protection Suite 8.8, Trendmicro 10.6.3, Symantec Endpoint Protection 12.1.4; Kaspersky Endpoint Security 10.2.2.10535.

• *Поддержка Kerberos*. Система WinCC OA поддерживает использование протокола Kerberos, позволяющего обеспечить взаимную идентификацию серверов и клиентов, а также ЭЦП или шифрование передаваемых сообщений.

• *Защищенная Web-публикация*. Система WinCC OA поддерживает взаимодействие с клиентами также и через Web. Web-страницы, отображающие процесс, публикуются при помощи HTTP-сервера WinCC OA, находящегося в демилитаризованной зоне (ДМЗ), и защищаются от внешних атак посредством внешнего межсетевого экрана. Дополнительная защита обеспечивается путем подмены идентификаторов. Трансляция адресов и изменение имен Web-серверов позволяют избежать прямого доступа к серверам. Внешний межсетевой экран выступает в качестве "авторизованного представителя" Web-сервера. Топология и IP-адреса ДМЗ непрозрачны для внешней сети. Динамический, зависящий от состояния контроль обмена данными на уровне приложений, совмещенный с фильтрами пользовательских приложений, команд и данных, осуществляется при каждом индивидуальном запросе Web-страницы.

• *Использование мультиплексного прокси и ограничение перечня открытых портов и списка разрешенных IP-адресов*. Преимуществом использования прокси является существенное сокращение числа открываемых на межсетевом экране портов. На рис. 7 схематично представлено решение для защищенной Web-публикации с использованием мультиплексного прокси, HTTP-сервера WinCC OA расположены в ДМЗ. Мультиплексные прокси функционируют на серверах WinCC OA. При подобном архитектурном решении на нижнем межсетевом экране требуется открытие только одного порта.

• *Использование TLS/SSL при информационном обмене*. При наличии мультиплексного прокси WinCC OA по умолчанию в каждом проекте взаимодействие осуществляется с использованием TLS/SSL, что позволяет обеспечить защищенную коммуникацию без применения Kerberos. В WinCC OA имеется конфигурационная панель, позволяющая создавать сертификаты, основанные на openSSL. Дополнительная информация о создании собственных сертификатов и поддерживаемой версии openSSL приведена в справке по WinCC OA.

• *Запрещение автоматической разблокировки мобильных устройств (Android and iOS)*. WinCC OA пре-

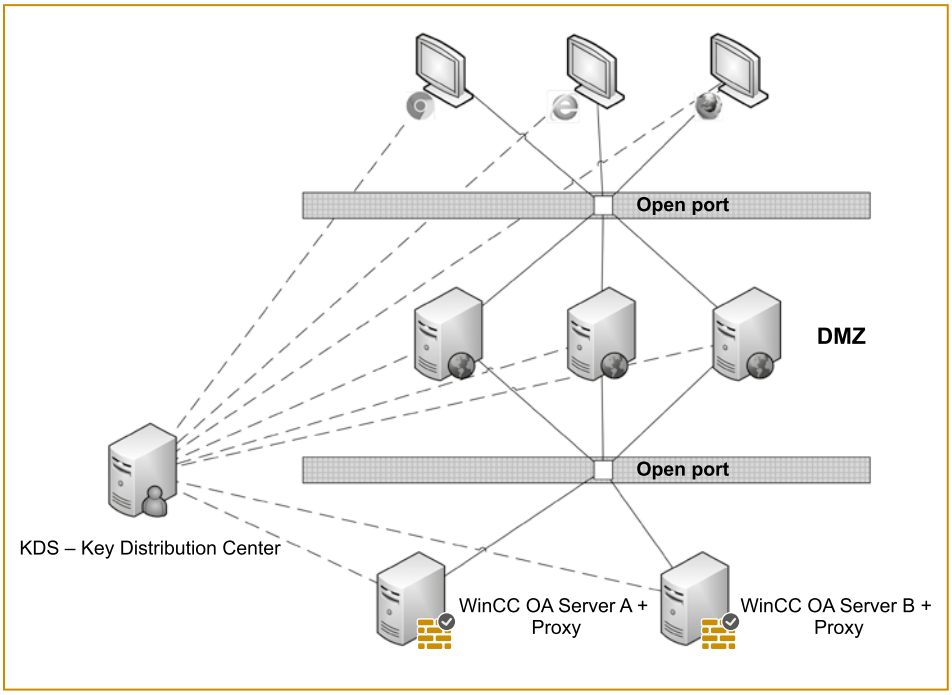

Рис. 7. Решение для защищенной Web-публикации с использованием мультиплексного прокси

доставляет интерфейсы к устройствам с ОС Android и iOS. С целью упрощенного подключения новых устройств опция автоматической разблокировки новых устройств автоматически активируется в проекте WinCC OA при создании проекта. Для повышения уровня безопасности имеется возможность запрещения автоматической разблокировки мобильных устройств. Если автоматическая разблокировка мобильных устройств запрещена, для подключения каждого нового устройства требуется непосредственное участие администратора системы.

• *Активация шифрования в WinCC OA и в Oracle*. Любая информация, передаваемая между двумя компьютерами, может быть достаточно легко перехвачена и использована для нанесения вреда компании. В этой связи рекомендуется использование шифрования передаваемых данных. При использовании Kerberos совместно с WinCC OA шифрование может быть активировано при помощи записи в конфигурационном файле (kerberosSecurity = “enc”).

Менеджер архива РБД WinCC OA взаимодействует с клиентом Oracle и направляет данные серверу Oracle. Для предотвращения перехвата информации и использования ее во вредоносных целях рекомендуется активация шифрования Oracle. При установке подключения к Oracle дополнительно рекомендуется использование однократной идентификаций (Single Sign On).

• *Запуск проекта WinCC OA в качестве сервиса*. Дополнительное повышение защищенности может быть обеспечено путем запуска проекта WinCC OA в качестве сервиса от имени системной учетной записи или от имени учетной записи определенного пользователя. Подобный подход позволяет ограничить доступ проекта к определенным ресурсам. При этом добавляется еще один уровень безопасности. Доступ к файлам и ресурсам ограничен полномочиями, предоставленными пользователю, от имени которого запускается сервис.

Заключение

Данная статья представляет собой лишь краткий обзор выборочных организационных и технических мер, принципов и встроенных механизмов обеспечения информационной безопасности при применении SCADA-системы SIMATIC WinCC Open Architecture. Более подробная информация для реализации организационных мероприятий описана в указанных выше нормативных документах. Подробнее о встроенных механизмах обеспечения безопасности SIMATIC WinCC Open Architecture изложено в "Концепции обеспечения безопасности SIMATIC WinCC Open Architecture» (www.etm.at).

Список литературы

1. *Соловьёв С.Ю., Космин А.С.* Построение распределённых систем сбора и обработки данных на базе платформы WinCC OA // ИСУП. 2015. № 4 (58).
2. *Соловьёв С.Ю., Серов А.Ю.* Новые возможности дистанционного мониторинга и управления промышленными и инфраструктурными объектами с помощью WinCC OA версии 3.15 // ИСУП. 2017. № 1.
3. *Colbert Ed. J. M., Kott Al.* Cyber-security of SCADA and Other Industrial Control Systems. Springer. 2016.

Мельников Андрей Сергеевич *– гл. инженер по интеграции проекта,*
Соловьев Сергей Юрьевич *– канд. техн. наук, руководитель группы,*
департамент «Цифровое производство», ООО «Сименс».
Контактный телефон +7 (495) 737-24-41.
E-mail: dfpd.ru@siemens.com
Http://siemens.ru

Компания Сименс оснастила электробус нового поколения для Москвы

В конце 2016 г. «Группа ГАЗ» представила электробус нового поколения, разработанный при участии МГТУ им. Н.Э. Баумана и компании Сименс.

Машина создана на базе городского низкопольного автобуса ЛиАЗ-5292. Проект является первым совместным комплексным решением интеграции европейских и российских технологий в области создания электрического автотранспорта в нашей стране. В прототипе электробуса применяется программное обеспечение и современный тяговой привод ELFA2 производства Сименс, отличающийся энергоэффективностью и низкими эксплуатационными затратами. Компания уже имеет опыт создания электробусов, которые в настоящее время успешно используются в Норвегии, Нидерландах, Великобритании, Индии и Китае.

Работа по оснащению электробуса шла в рамках соглашения о сотрудничестве, подписанного между Правительством Москвы и Сименс в июне 2016 г. Специалистами компании были проведены инжиниринговые работы, произведена адаптация оборудования к инфраструктуре автобуса, успешно завершен пуско-наладочный процесс. При этом сохранен высокий уровень унификации электробуса с модельной линейкой Ликинского автобусного завода «Группы ГАЗ», что позволяет достичь максимальной экономической эффективности для перевозчика в части затрат на обслуживание техники.

Опытный образец рассчитан на перевозку до 90 пассажиров и имеет 27 посадочных мест с возможностью крепления трех кресел для пассажиров с ограниченными возможностями. Электробус получил международный экологический стандарт Zero Emission, который характеризуется полным отсутствием вредных выбросов в атмосферу. Концепция нового электробуса разработана при участии научной школы МГТУ им. Н.Э. Баумана. Электробус укомплектован литий-марганцевыми батареями, имеющими высокую энергоемкость и обладающими повышенным жизненным ресурсом – до 5 тыс. циклов зарядки/разрядки, что позволяет при использовании модульного решения по зарядке увеличить суточный пробег машины до 200 км. Реализация этого решения подразумевает длительную ночную зарядку электробуса и 2...3 короткие подзарядки в течение 20...30 мин на конечных точках маршрута.

В июне 2017 г. в рамках Петербургского международного экономического форума компании «Сименс АГ» и ОАО «ВНИИР» (группа компаний «АБС Электро») подписали соглашение о намерениях по совместной работе в проектах по созданию зарядной инфраструктуры для электробусов в России.

https://www.siemens.ru