Обеспечение безопасности SCADA-системы WinCC OA средствами WinCC OA и KICS

А.С. Мельников (ООО «Сименс»),
С.И. Палтов (АО «Лаборатория Касперского»)

Приводится сопоставление указанных в Приказе ФСТЭК от 25.12.2017 N 239 мер по обеспечению безопасности значимых объектов и функции безопасности SCADA-системы SIMATIC WinCC Open Architecture и решения по безопасности Kaspersky Industrial CyberSecurity, которые могут быть использованы при реализации данных мер.

Ключевые слова: информационная безопасность, кибербезопасность, SCADA-система, мониторинг промышленных сетей, объект критической информационной инфраструктуры.

SCADA-система SIMATIC WinCC Open Architecture (WinCC OA) входит в семейство продуктов SIMATIC HMI и предназначена для решения задач сбора и обработки данных, а также для решения задач управления и визуализации.

В связи с представленными ниже принципами построения и основными особенностями система WinCC OA идеально подходит для создания простых односерверных приложений, крупномасштабных и/или сложных приложений, для интеграции систем от различных производителей, а также для построения географически распределенных систем. При этом система обладает огромными возможностями по расширению и масштабированию и позволяет обеспечивать выполнение самых высоких требований к надежности и безопасности.

Система построена по модульному принципу и состоит из менеджеров — функциональных единиц системы, программно реализованных в виде отдельных процессов. Взаимодействие менеджеров между собой осуществляется по TCP/IP (рис. 1).

Некоторые менеджеры (например, драйверы или пользовательские интерфейсы) могут запускаться на отдельных удаленных компьютерах, что позволяет балансировать нагрузку на вычислительные ресурсы и сеть. Какие-либо действия в системе и обмен данными осуществляются в основном по событиям, что в целом также приводит к более эффективному использованию ресурсов.

Основные особенности WinCC OA:

- объектно-ориентированный подход к инжинирингу;
- возможность создания распределенных систем с поддержкой до 2048 серверов;
- масштабируемость от одиночной системы до распределенных резервированных высокопроизводительных систем, обрабатывающих более 10 млн. сигналов ввода/вывода;
- возможность применения на различных платформах (ОС Windows, Linux, iOS и Android);
- горячее резервирование и резервирование по схеме 2×2 (“катастрофоустойчивая система”);
- наличие пакетов расширения функциональности (ГИС, видео, аналитика, рецептурное управление и др.);

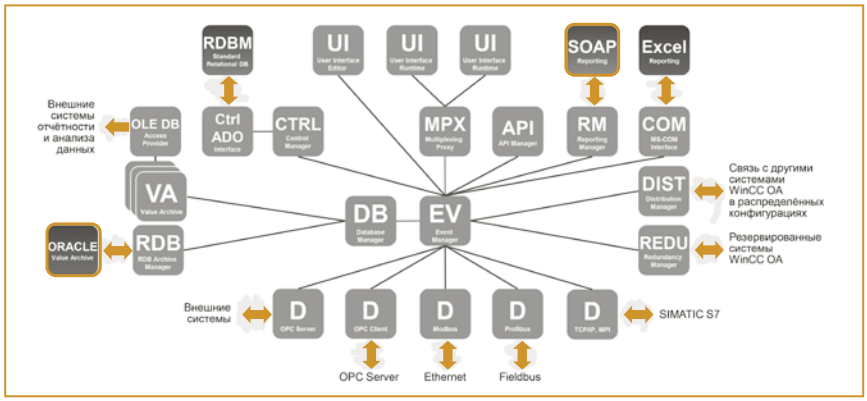


Рис. 1. Модульный принцип построения системы WinCC OA

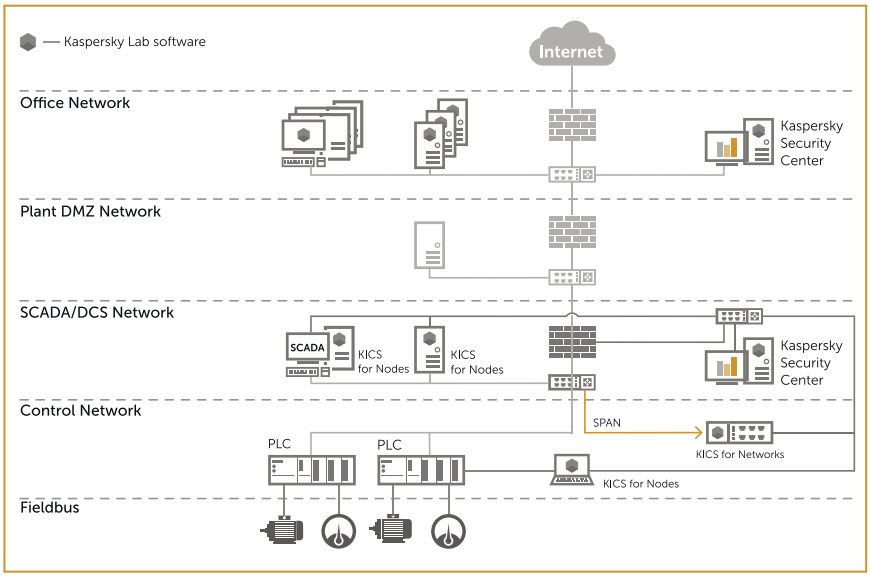


Рис. 2. Развертывание компонентов Kaspersky Industrial CyberSecurity

Таблица. Сопоставление приведенных в приказе ФСТЭК N 239 блоков мер по обеспечению безопасности объектов и функций WinCC OA, KICS for Nodes и KICS for Networks, которые могут быть использованы для реализации данных мер

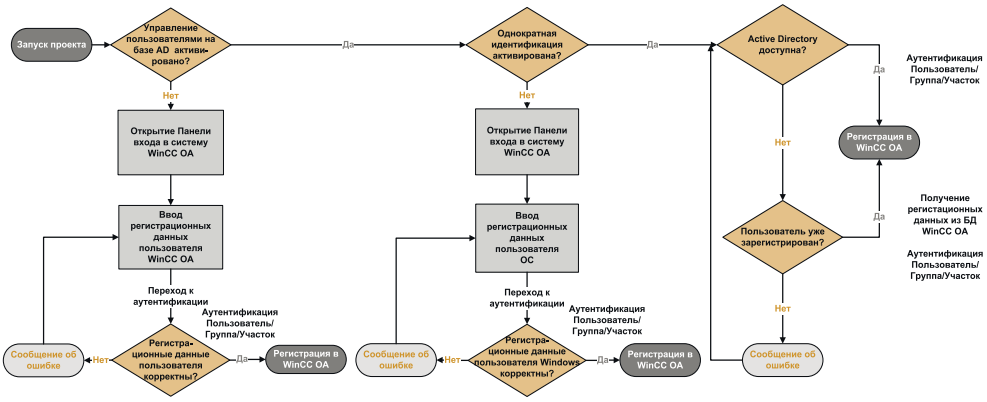
<table>
<tr><th>Функции WinCC OA и KICS, которые могут быть использованы при реализации мер по обеспечению безопасности значимого объекта</th><th>Блоки мер по обеспечению безопасности значимого объекта согласно Приказу ФСТЭК N 239</th></tr>
<tr><td>WinCC OA Применимость к компонентам SCADA-системы: уровень SCADA (WinCC OA)</td><td></td></tr>
<tr><td>Управление идентификаторами и аутентификаторами. В качестве идентификаторов и аутентификаторов используются имена пользователей и пароли. Возможно независимое управление идентификаторами и аутентификаторами на уровне WinCC OA, а также интеграция с Active Directory (AD) или внешним LDAP.</td><td rowspan="3">Идентификация и аутентификация, управление доступом</td></tr>
<tr><td>Идентификация и аутентификация пользователей по именам пользователей и паролям</td></tr>
<tr><td>Однократная аутентификация. При запуске клиента WinCC OA происходит автоматический вход в систему WinCC OA от имени учетной записи в AD, которая использовалась при регистрации на уровне ОС рабочей станции. Функция может использоваться только при интеграции с AD. Применение данной функции наиболее эффективно в комбинации с автоматическим запуском клиента WinCC OA после регистрации пользователя на уровне ОС, поскольку при блокировании соответствующих функций ОС (горячих клавиш и т.п.) исключается возможность совершения оператором каких-либо действий на уровне ОС (рис. 3).
 

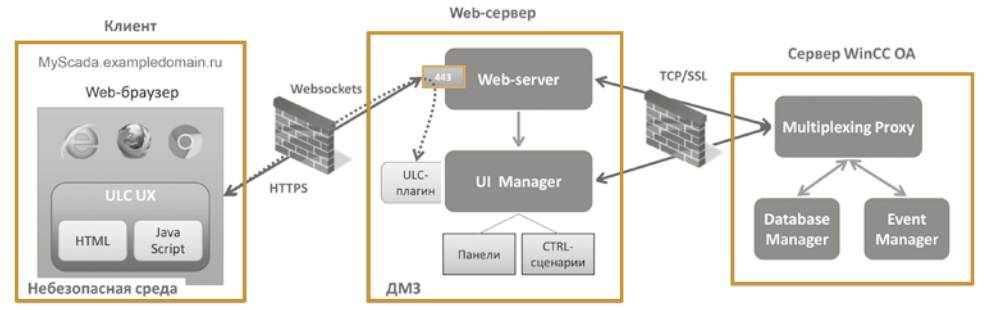
Рис. 3. Алгоритм однократной аутентификации в системе WinCC OA</td><td></td></tr>
<tr><td>Аутентификация менеджеров на стороне сервера (аутентификация менеджеров, например, драйверов, запускаемых на удаленных хостах, с использованием сертификатов PKI)</td><td>Идентификация и аутентификация, управление доступом, ограничение программной среды</td></tr>
<tr><td>Управление полномочиями пользователей. Пользователи включаются в одну или несколько групп (членство в группах настраивается на уровне WinCC OA, синхронизируется с AD или внешним LDAP). Полномочия всегда задаются на уровне групп пользователей WinCC OA. Возможно ограничение полномочий для рабочих станций и участков WinCC OA. Доступны следующие стандартные уровни полномочий: визуализация (допускается отображение объекта), базовые права пользователя (допускается открытие панелей), расширенные права пользователя, администрирование, квитирование (алармов). Возможна настройка дополнительных уровней.</td><td rowspan="5">Управление доступом, защита информационной (автоматизированной) системы и ее компонентов</td></tr>
<tr><td>Конфигурационные элементы "_auth ". Гранулированная настройка полномочий на операции с отдельными атрибутами тэгов. Атрибутами тэгов являются, например, формат значений, аларм-диапазон, текущее значение и т.п.</td></tr>
<tr><td>Подключаемый модуль контроля доступа обеспечивает ограничение доступа менеджера (например, пользовательского интерфейса) к указанным тэгам.</td></tr>
<tr><td>Мультиплексный прокси-сервер WinCC OA - менеджер WinCC OA для организации туннелей SSL к другим удаленным менеджерам. Для туннеля требуется только один открытый порт на внешнем межсетевом экране (МСЭ). Обеспечивается блокирование DoS-атак.</td></tr>
<tr><td>Защищенная Web-публикация. Безопасное подключение клиентов ULC UX. Подключение осуществляется по HTTPS. Используется HTML5. Web-сервер WinCC OA устанавливается в демилитаризованной зоне (ДМЗ). (рис. 4).
 

Рис. 4. Безопасное подключение клиентов ULC UX в системе WinCC OA</td></tr>
<tr><td>Защищенная Web-публикация. Безопасное подключение клиентов для iOS и Android. Подключение осуществляется по SSL и HTTPS. Web-сервер WinCC OA устанавливается в ДМЗ.</td></tr>
</table>

Таблица. Сопоставление приведенных в приказе ФСТЭК N 239 блоков мер по обеспечению безопасности объектов и функций WinCC OA, KICS for Nodes и KICS for Networks, которые могут быть использованы для реализации данных мер (продолжение)

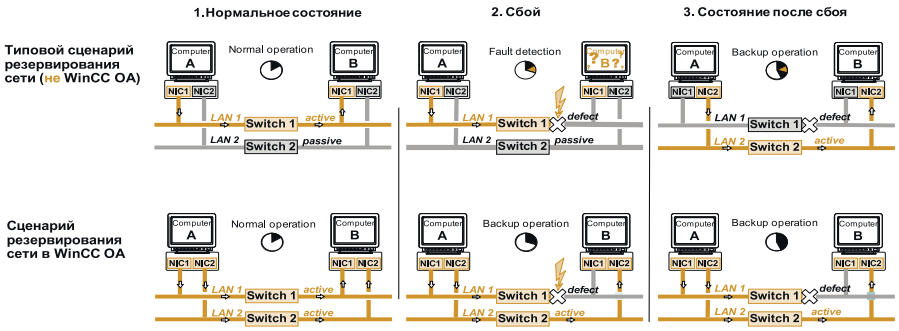
Автоматический выход из системы (при неактивности). Возможна также блокировка экрана, выключение ПК и т.п.	Управление доступом
Смена пользователя без закрытия экранной формы. При выходе пользователя из системы технологический процесс продолжает отображаться на экране, однако последующее управление процессом станет возможным только при входе в систему пользователя с достаточным уровнем полномочий.	
Настройка процесса пользовательской аутентификации, включая диалоговые окна и уведомления при входе в систему	
Запуск проекта WinCC OA в качестве сервиса Windows/Linux (с требуемыми полномочиями на уровне ОС)	
Фиксированное лицензирование (привязка лицензий, в том числе администраторов WinCC OA к конкретным рабочим местам)	Управление конфигурацией
Обновления для системы WinCC OA доступны на портале https://www.winccoa.com/ после заказа обязательного сопровождения	Управление обновлениями программного обеспечения
Журналирование событий безопасности и системных событий. Журналирование действий оператора может быть обеспечено с применением внутреннего языка Control.	Аудит безопасности, предотвращение вторжений (компьютерных атак), обеспечение целостности
Совместимость с антивирусным ПО, в т.ч. с антивирусом в составе KICS.	Антивирусная защита
Горячее резервирование серверов WinCC OA (обеспечивается бесшовное переключение на резервный сервер)	Обеспечение доступности, обеспечение действий в нештатных ситуациях
Резервирование сетевых подключений. Система WinCC OA одновременно отправляет два идентичных сообщения по двум физически или логически различным сетям. В случае работоспособности обеих сетей, на стороне принимающей системы WinCC OA последнее пришедшее сообщение отбрасывается. В случае отказа одной из сетей одно из двух одновременно отправленных сообщений в любом случае будет доставлено до принимающей системы WinCC OA и обработано (рис. 5).  Рис. 5. Резервирование сетевых подключений в системе WinCC OA	
Катастрофоустойчивая система - резервирование по схеме 2x2. Обеспечивается бесшовное переключение на резервный сервер в рамках центра управления или на резервный центр управления (рис. 6).	
Резервное копирование и восстановление текущих значений тэгов, архивов значений и алармов, а также собственно проекта	
Шифрование сценариев и панелей. Зашифрованные сценарии и панели передаются разработчиком проекта заказчику. Проект запускается на выполнение без ограничений, однако изменение и чтение зашифрованных панелей и сценариев невозможны.	Защита информационной (автоматизированной) системы и ее компонентов
Запрещение автоматической разблокировки мобильных устройств (обеспечение возможности подключения только явно указанных клиентов)	
Поддерживаемые ОС и приложения (в т.ч. для создания гетерогенной среды Windows, RedHat, CentOS, OpenSUSE Leap, Oracle Server, Oracle Client, VMware ESXi, vSphere HA Cluster)	
Поддерживаемые мобильные ОС и браузеры (в т.ч. для создания гетерогенной среды iOS, Android, Microsoft IE, Microsoft EDGE, Firefox, Chrome)	
Поддержка Kerberos - взаимная идентификация серверов и клиентов, а также ЭЦП или шифрование передаваемых сообщений.	
Разработка на внутреннем языке Control - дополнительные алгоритмы и функции могут быть реализованы с использованием внутреннего языка программирования Control.	Управление доступом, аудит безопасности, обеспечение целостности, обеспечение доступности
Подписка на изменения структуры тэгов	Обеспечение целостности
Метки времени и синхронизация системного времени. Все события в WinCC OA регистрируются с метками времени. При формировании меток времени используется системное время ОС.	Аудит безопасности
Siemens CERT. Информация об обнаруженных уязвимостях в системе WinCC OA и способах их устранения доступна на странице службы Siemens CERT, https://www.siemens.com/global/en/home/products/services/cert.html	
KICS for Nodes Применимость к компонентам SCADA-системы: уровень ОС	
Application Launch Control обеспечивает формирование белого списка исполняемых файлов, файлов установки, драйверов и скриптов на основе цифровых сертификатов и контрольных сумм файлов и допускает контроль их запуска/загрузки в режиме статистики или блокирования по умолчанию.	Ограничение программной среды, аудит безопасности, предотвращение вторжений (компьютерных атак), обеспечение целостности
Device Control контролирует регистрацию и использование съемных запоминающих устройств и устройств чтения CD/DVD на основе списка доверенных устройств и допускает работу в двух режимах: статистика и активная блокировка.	Аудит безопасности, предотвращение вторжений (компьютерных атак), защита машинных носителей информации

Таблица. Сопоставление приведенных в приказе ФСТЭК N 239 блоков мер по обеспечению безопасности объектов и функций WinCC OA, KICS for Nodes и KICS for Networks, которые могут быть использованы для реализации данных мер (окончание)

Real-Time File Protection реализует стандартные функции защиты узлов от вредоносного ПО (например, вирусов), в т. ч. функции, позволяющие использовать неблокирующий режим (не является рекомендованным)	Аудит безопасности, антивирусная защита, предотвращение вторжений (компьютерных атак)
Anti-Cryptor - защита сетевых файловых ресурсов, размещаемых на защищаемых узлах, от воздействий вредоносного шифрования путем блокирования сетевой сессии источника шифрования.	
Untrusted Host Blocker - блокирование сетевых подключений со стороны узлов, проявляющих признаки вредоносной деятельности, например, признаки распространения вредоносного ПО по сети.	
Wi-Fi Control контролирует подключения устройств к беспроводным сетям, ограничивая защищаемое устройство возможностью подключения только к доверенным сетям и допускает режим только уведомления или блокирования подключений.	Защита информационной (автоматизированной) системы и ее компонентов
Firewall Management - механизм реализует функцию централизованного управления запуском и настройками межсетевого экрана ОС.	Аудит безопасности, предотвращение вторжений (компьютерных атак), защита информационной (автоматизированной) системы и ее компонентов
File Integrity Monitor - отслеживание файловых операций в настраиваемых областях файловой системы.	Аудит безопасности, предотвращение вторжений (компьютерных атак), обеспечение целостности
Log Inspection - отслеживание событий в журналах ОС, информирование о возникновении подозрительных событий на основе эвристического анализа или выявления идентификаторов событий.	Аудит безопасности, предотвращение вторжений (компьютерных атак)
Exploit Prevention - защита процессов от эксплуатации уязвимостей и внедрения стороннего кода, допускает режим предотвращения и уведомления о подозрительной активности.	
Trusted Zone - возможность определения областей файловой системы защищаемого узла, которые будут исключены из зоны действия файлового антивируса – используется для оптимизации производительности по рекомендации производителя ПО.	Антивирусная защита
Trusted Processes - возможность определения списка доверенных служб, файловые операции которых не будут перехватываться файловым антивирусом – используется для оптимизации производительности.	
Синхронизация системного времени - при формировании меток времени KICS for Nodes использует системное время ОС.	Аудит безопасности
Event List - журналирование событий безопасности. События безопасности записываются в зашифрованный журнал KICS for Nodes, расположенный на защищаемом узле, и в системные журналы Windows (опционально). При использовании KSC события безопасности передаются на уровень KSC с применением шифрования.	
Centralized Management - централизованное обновление антивирусных сигнатур, а также централизованное управление настройками безопасности.	-
KICS for Nodes Применимость к компонентам SCADA-системы: уровень ПЛК	
PLC Integrity Check - контролирует неизменность управляющей программы ПЛК, периодически сопоставляя контрольную сумму актуальной программы с эталонной, полученной в ходе первоначальной настройки.	Аудит безопасности, предотвращение вторжений (компьютерных атак), управление конфигурацией
KICS for Networks Применимость к компонентам SCADA-системы: уровень сети	
Asset detection - механизм пассивного обнаружения передающих устройств сети Ethernet, реализуемый путем анализа копии сетевого трафика, снимаемого с коммутатора или концентратора сети Ethernet. Предоставляется возможность автоматического создания списка известных устройств и их свойств («белого списка») и последующего обнаружения новых устройств или изменений в конфигурации известных с формированием соответствующих оповещений.	Аудит безопасности, предотвращение вторжений (компьютерных атак), управление конфигурацией
Intrusion Detection System - механизм пассивного обнаружения вредоносной или подозрительной сетевой активности с формированием соответствующих оповещений.	Аудит безопасности, предотвращение вторжений (компьютерных атак)
Deep Packet Inspection - механизм пассивного обнаружения в сетевом трафике параметров технологического процесса на основе анализа протоколов прикладного уровня технологических систем с формированием соответствующих оповещений.	Аудит безопасности, предотвращение вторжений (компьютерных атак), защита информационной (автоматизированной) системы и ее компонентов, управление конфигурацией
Command Control - механизм пассивного обнаружения в сетевом трафике системных команд, используемых при работе с контроллерами (например, команд на изменение управляющей программы ПЛК или на перезагрузку ПЛК), Предоставляется возможность автоматического создания профиля типовых команд и их узлов-участников («белого списка») и последующего обнаружения отклонений от профиля с формированием соответствующих оповещений.	
Process Control - функция отслеживания значений технологических параметров и их комбинаций, реализованная на основе данных технологических протоколов с использованием механизма *Deep Packet Inspection*. В случае выхода значений технологических параметров за настроенные границы формируются соответствующие оповещения.	
Network Integrity Control - механизм пассивного обнаружения сетевых взаимодействий между узлами сети Ethernet. Обнаружение сетевых коммуникаций реализуется путем анализа копии сетевого трафика, снимаемого с коммутатора или концентратора сети Ethernet. Предоставляется возможность автоматического создания профиля разрешенных сетевых коммуникаций («белого списка») и последующего обнаружения отклонений от него с формированием соответствующих оповещений.	
Circular buffer - копия сетевого трафика, сохраняемая системой с целью последующего возможного анализа/ расследования инцидентов информационной безопасности.	Аудит безопасности, защита информационной (автоматизированной) системы и ее компонентов, управление конфигурацией
Синхронизация системного времени - при формировании меток времени KICS for Networks использует системное время ОС.	Аудит безопасности
Event List - события безопасности записываются в журнал KICS for Networks, расположенный на сервере. При использовании KSC события безопасности также передаются на уровень KSC с применением шифрования.	
Centralized Management - возможность централизованного управления настройками безопасности.	-

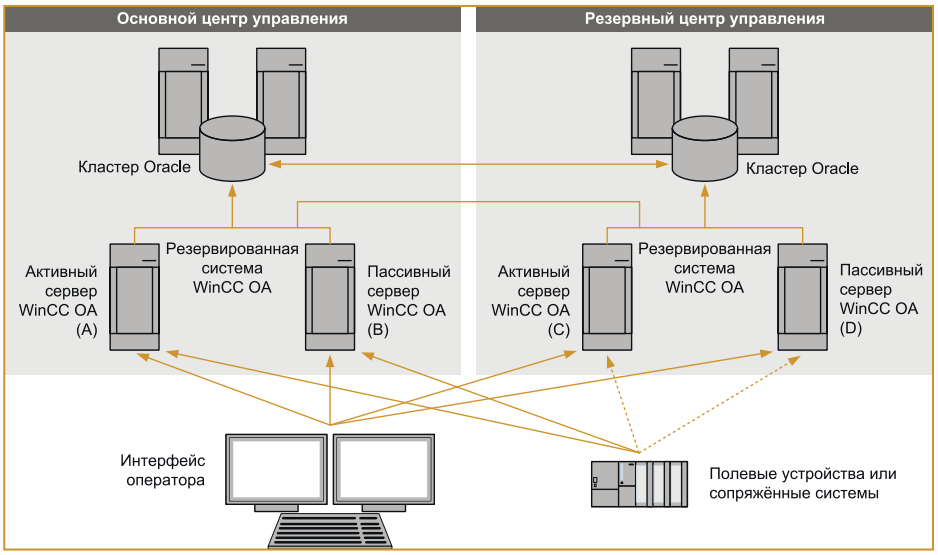


Рис. 6. Архитектура WinCC OA с резервированием 2x2

• платформа для разработки индивидуальных и специализированных решений;

• широкий спектр поддерживаемых протоколов обмена данными: SIMATIC S7 Plus, SIMATIC S7, XML, OPC, OPC UA, TCP/IP, Modbus, IEC 60870-5-101/104, DNP3, IEC 61850, IEC 61400, Ethernet/IP, S-Bus и др. [1]

Благодаря гибкой концепции построения WinCC OA находит применение практически во всех отраслях промышленности и на самых разных инфраструктурных объектах — от систем управления движением, сетей водо- и газоснабжения, нефтепроводов и до центров ядерных исследований [1].

На сегодняшний день география внедрений системы WinCC OA охватывает все континенты, при этом более 7000 проектов относятся к разряду крупных.

В качестве крупных объектов на территории РФ отметим Камскую ГЭС, Саяно-Шушенскую ГЭС, системы диспетчерского контроля и управления и измерения количества и показателей качества нефти и нефтепродуктов (СИКН) ПАО «Транснефть», систему диспетчеризации центральной производственно-диспетчерской службы ОАО «Арктикгаз», систему измерения количества газа на газопроводе от ГРС-2 (г. Нижнекамск) до потребителей ОАО «ТАИФ-НК» и др. Общее число внедрений системы WinCC OA на территории РФ неуклонно растет.

Многие объекты, на которых используется система WinCC OA, относятся к значимым объектам критической информационной инфраструктуры. Для них с 1 января 2018 г. действует ФЗ "О безопасности критической информационной инфраструктуры РФ" от 26.07.2017 N 187-ФЗ и соответствующие подзаконные акты, в частности, приказ ФСТЭК России от 25.12.2017 N 239 "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ".

Для выполнения многих мер по обеспечению безопасности объектов (в том числе приведенных в приказе ФСТЭК N 239) система WinCC OA поддерживает широкий спектр функций безопасности [2, 3], кумулятивно представленный в таблице.

Отметим, что “по историческим причинам” функции безопасности WinCC OA относятся к уровню приложения WinCC OA и сетевым подключениям между удаленными компонентами WinCC OA, а для обеспечения безопасности других компонентов SCADA-системы, например, операционной системы и сетевой инфраструктуры, может быть применено решение Kaspersky Industrial CyberSecurity (KICS). KICS представляет собой специализированное решение для обеспечения информационной безопасности критических инфраструктур. Это решение реализует функции комплексной защиты конечных узлов с помощью компонента KICS for Nodes и пассивный мониторинг промышленных сетей с помощью компонента KICS for Networks (рис. 2). Для централизованного управления настройками KICS, а также для сбора и анализа событий информационной безопасности рекомендуется использовать продукт Kaspersky Security Center (KSC). Помимо перечисленных функций, KSC может быть использован для выполнения задач интеграции со смежными системами, проведения инвентаризации ПО, установленного на рабочих станциях и серверах, поиска известных уязвимостей и централизованного распространения обновлений программных продуктов. Компоненты KICS сертифицированы ФСТЭК России и могут быть использованы при реализации требований ФЗ N 187-ФЗ и Приказа ФСТЭК N 239.Более подробный список функций, реализуемых решением Kaspersky Industrial CyberSecurity, представлен в таблице.

С целью предоставления заказчикам гарантированно совместимых продуктов, силами компаний “Лаборатория Касперского” и ETM professional control GmbH (дочерней компании Siemens AG) в феврале 2019 г. было проведено тестирование, подтвердившее возможность совместного использования и штатного функционирования продуктов Kaspersky Industrial CyberSecurity for Nodes 2.5, Kaspersky Industrial CyberSecurity for Networks 2.7 и WinCC OA 3.16 в единой среде. При этом в ходе указанного тестирования компоненты KICS разворачивались не только на простых односерверных архитектурах WinCC OA, но и на многосерверной архитектуре WinCC OA с резервированием 2x2 (рис. 6).

Заключение

Рассмотренные в настоящей статье функции безопасности WinCC OA и KICS могут быть использованы заказчиками из различных отраслей промышленности для обеспечения кибербезопасности эксплуатируемых и внедряемых систем промышленной автоматизации, диспетчерского контроля и управления. В данной статье приведена только сводная обзорная информация о данных функциях — для получения более детальных сведений целесообразно обратиться к “Справке по системе WinCC OA” (поставляется в составе демонстрационной версии, которая доступна на портале https://www.winccoa.com после регистрации), к пользовательской документации на продукты Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Networks (поставляется вместе с продуктами) или непосредственно к авторам данной статьи.

Список литературы

1. *Космин А.С., Серов А.Ю., Соловьев С.Ю.* Мониторинг производственных линий с SIMATIC WinCC Open Architecture // Control Engineering Россия. 2017. №6 (72).
2. *Мельников А.С., Соловьев С.Ю.* Обеспечение информационной безопасности при применении SCADA-Системы SIMATIC WINCC Open Architecture // Автоматизация в промышленности. 2017. №7.
3. *Серов А.Ю., Соловьев С.Ю.* Новое в WinCC OA версии 3.16: инженерная эффективность, производительность и безопасность как ключевые характеристики SCADA-системы в эпоху цифровой трансформации // ИСУП. 2018. № 3(75).

Мельников Андрей Сергеевич *– главный инженер по интеграции проекта ООО «Сименс»,*
Палтов Сергей Игоревич *– руководитель группы по развитию архитектуры решений АО «Лаборатория Касперского».*
Контактный телефон+7 (495) 737-1-737.
E-mail: winccoa.ru@siemens.com, icc.ru@siemens.com
http://dfpd.siemens.ru

Состояние и перспективы внедрения беспроводных технологий для IoT

Компания J’son & Partners Consulting представила результаты «Состояние и перспективы внедрения беспроводных технологий для IoT (LoRaWAN, SigFox, NB-IoT, LTE-M и др.)».

Для обеспечения подключения устройств IoT могут использоваться различные радиотехнологии и стандарты беспроводной связи. Предполагается, что значительное число устройств IoT (около 80%) будут подключены через шлюзы на основе локальных и персональных сетей в полосах радиочастот, используемых в упрощенном порядке. При этом сами шлюзы могут быть подключены через существующие сети сотовой подвижной связи или узкополосные беспроводные сети связи IoT.

Несмотря на то, что узкополосные беспроводные сети связи IoT не рассматриваются в качестве самого массового сегмента, их предполагается использовать для подключения устройств IoT во многих отраслях экономики для широкого ряда применений, которые будет затруднительно или невозможно реализовать с использованием других типов беспроводной связи.

Узкополосные беспроводные сети связи IoT в полосах радиочастот, используемых в общем порядке (в лицензируемом спектре), представлены несколькими стандартами, среди которых самыми распространенными являются NB-IoT и LTE-M консорциума 3GPP. Фактически эти технологии не являются самостоятельными стандартами, а представляют собой развитие существующих стандартов сотовой подвижной связи, доработанных для удовлетворения потребностей в подключении маломощных устройств, работающих, как правило, от батареи и имеющих ограниченные потребности в пропускной способности.

При этом существует более десятка различных открытых и закрытых стандартов узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в упрощенном порядке (в нелицензируемом спектре), но, прежде всего, по популярности в мире стоит выделить LoRaWAN и SigFox.

В настоящее время на российском рынке коммерчески доступны как устройства с поддержкой LoRaWAN, так и «локальные» российские технологии NB-Fi и XNB, а также сетевое оборудование (инфраструктура) для них. В ближайшей перспективе ожидается появление на рынке первых коммерческих устройств с поддержкой технологии NB-IoT.

В перспективе, по мере развития новых технологий (узкополосных LoRaWAN, NB-IoT и др., в более долгосрочной перспективе — 5G) операторы связи будут пытаться захватывать новые ниши, предлагая не только сервис связи как таковой, но и комплексное решение, включая услуги системной интеграции и сервисных IoT-платформ. Эта тенденция уже наметилась.

Стандарты 3GPP для новых радиосетей (New Radio, NR), способных работать вместе с существующими сетями LTE, в которых используется неавтономный режим (non-standalone, NSA) для подвижной сверхширокополосной связи, были согласованы в декабре 2017 г. Стандарты 3GPP Релиз 15 для автономного (standalone, SA) режима 5G NR были завершены в июне 2018 г. Ожидается дальнейшая эволюция стандартов 5G в 16-м релизе 3GPP, принятие которого планируется в начале 2020 г.

По мере того, как телекоммуникационная отрасль стремительно приближается к коммерческому внедрению технологии 5G, существенно растет число операторов, инвестирующих в такие технологии. Операторы со всех континентов заявляют об участии в демонстрациях 5G, лабораторных и полевых испытаниях. Многие из них объявили о планах по запуску услуг 5G, а некоторые уже запустили коммерческие сервисы. По оценкам GSA, более 200 операторов в 83 странах активно инвестируют в 5G.

К началу июля 2019 г. коммерческие сети 5G с поддержкой смартфонов были запущены в Южной Корее, США, Австралии, Швейцарии, Великобритании и Германии.

В России, в соответствии с паспортом национальной программы «Цифровая экономика РФ», до конца 2020 г. должны быть реализованы лишь пилотные проекты по созданию сетей связи 5G, а до конца 2021 г. — созданы условия для развертывания таких сетей на территории не менее 10 городов-миллионников. В проекте целевой программы Минпромторга указано, что развертывание сетей 5G в России начнется в 2022 г. и продлится не менее 10 лет. При этом основным сдерживающим фактором развития сетей 5G в России является дефицит частотного ресурса.

Http://json.tv