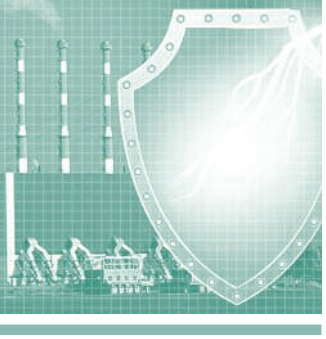

Индустриальная революция и кибербезопасность

Ольга Киселёва, Юрий Широков

«Кто владеет информацией, тот владеет миром» – эта крылатая фраза Натана Ротшильда сейчас актуальна, как никогда ранее. В современном мире данных становится всё больше, и выигрывает конкурентную борьбу тот, кто может не только грамотно собрать и проанализировать полученную информацию, но и обезопасить свои данные, используя надёжные системы для защиты от кибердударов и сетевых «зловредов». В этой статье речь идёт о современных технологиях, используемых для АСУ ТП и АСУП в рамках концепции текущей индустриальной революции, о вариантах защиты от киберугроз в пределах этих технологий, а также приведены рекомендации ведущих игроков этого рынка – компаний ICONICS и «Лаборатория Касперского» – по защите промышленных объектов.

На 80-е годы прошлого века пришёлся бум персональных компьютеров. Их массовая доступность спровоцировала рождение множества вирусных программ, а позже, с появлением и распространением коммерческого Интернета, создатели вирусов и их детища по-настоящему вышли на мировую арену. Но даже тогда авторы вирусных кодов ещё не воспринимались всерьёз. Да и сами «шутники» не ставили целей спровоцировать глобальный финансовый кризис или катастрофу с человеческими жертвами. Никто и представить себе не мог масштабов угрозы, с которой предстояло столкнуться всего лишь спустя несколько десятилетий.

В современном мире всё зиждется на данных. Данные сегодня собирают повсеместно: их хранят, передают и обрабатывают правительственные, коммерческие, медицинские, финансовые учреждения. Создаются наборы огромных объёмов личных данных граждан, пользователей, клиентов, сотрудников. Утечка и искажение этой информации могут повлечь весьма нежелательные последствия. Но гораздо бóльшую потенциальную угрозу представляет несанкционированный доступ злоумышленников к промышленным системам автоматизации. Здесь речь идёт уже о серьёзных последствиях вплоть до искусственно спровоцированных аварий и техногенных катастроф, чему есть реальные примеры. Поскольку практически всё сейчас управляется при помощи компьютеров, под кибердар легко могут попасть объекты и организации, обеспечивающие жизненно важную инфраструктуру города и даже страны.

Новые технологии – новые угрозы

Как ни парадоксально, многие технологические инновации последнего времени не только облегчают нам жизнь, но и создают новые опасности, поскольку попадают под прицел злоумышленников. Индустриальные компьютерные системы стремительно развиваются и порождают новые возможности. Сегодня автоматизированные системы передовых разработчиков используют технологии, радикально повышающие эффективность, удобство, надёжность. Вот некоторые из них.

Цифровые близнецы

Несмотря на то что цифровые близнецы, или цифровые двойники – понятие достаточно новое, сама концепция далеко не нова. По своей сути цифровой близнец – это виртуальная копия физического объекта, возможно полно симулирующая его поведение в различных условиях. Благодаря многочисленным сенсорам эта модель получает в реальном времени данные о текущем состоянии объекта и таким образом постоянно синхронизируется с ним. Цифровая модель может пригодиться во множестве случаев. Для начала с её помощью вы можете гораздо более глубоко проанализировать работу своей физической системы, не вмешиваясь в её функционирование. Задав виртуальной модели соответствующие параметры, можно провести анализ «что – если» и смоделировать нежелательные ситуации на реальном объекте. А если ваш близнец наделён функциональностью искусственного интеллекта, то он на основании накопленных статистических данных даст рекомендации по предотвращению возможных негативных сценариев развития событий и оптимизирует работу своего «брата». Имея цифрового близнеца производственной линии, можно виртуально дополнить её новым оборудованием и, только убедившись в совместимости, с полной уверенностью приобрести новый станок. Крайне востребована эта технология в транспортной и складской логистике, где такое моделирование может иметь просто потрясающий оптимизационный эффект. В настоящее время с развитием IIoT, беспроводных и облачных технологий, повышением производительности, удешевлением компьютеров и совершенствованием алгоритмов искусственного интеллекта концепция двойников бурно развивается и сулит захватывающие перспективы. Уже сегодня технология рассматривается как неотъемлемая часть реализации Индустрии 4.0.

Виртуальная и дополненная реальность

Виртуальная (от лат. virtualis – возможный) реальность – это искусственно созданный мир, который человек воспринимает посредством ощущений: зрения, слуха, обоняния, осязания. Су-

ществует также понятие «дополненная реальность» (augmented reality, AR), которое предполагает расширение возможностей восприятия путём введения в поле органов чувств человека дополнительной информации от различных сенсоров. Таким образом, виртуальная реальность – это полностью симулированный мир, в то время как дополненная реальность – лишь «усовершенствованная» версия реального мира. Технологию дополненной реальности сегодня активно используют военные (пример – шлем пилота), приходит она и в индустриальный мир АСУ ТП через интеграцию в SCADA-системы.

Облачные сервисы и мобильные устройства

С развитием облачных сервисов и беспроводных технологий применение мобильных устройств в системах промышленной автоматизации стало массовым. Мобильные устройства востребованы прежде всего сервисными и инженерными службами предприятий, которым они обеспечивают оперативность и удобство обслуживания. На экране планшета можно отобразить любую техническую информацию, а сервисы push-уведомлений позволяют не пропустить важное событие. Таким образом, оснащённый мобильными устройствами технический персонал имеет возможность обслуживать даже удалённые и распределённые объекты.

Ложка дёгтя

С точки зрения киберугроз, перечисленные технологии – своеобразная ложка дёгтя в бочке мёда: например, цифровой двойник, «живущий» в киберпространстве, является заманчивой мишенью для киберпреступников. И чем в большей степени мы полагаемся на виртуальные модели, тем реальнее опасность для физических объектов. Системы автоматизации становятся распределёнными и частично уходят в облака. Это также делает их инфраструктуру уязвимой для кибератак. Для облегчения обслуживания и повышения оперативности на компьютеры систем АСУ ТП часто устанавливаются программы удалённого администрирования (RAT).

Широкое распространение беспроводных технологий вкупе с несоблюдением мер защиты также облегчает подключение злоумышленников к промышленным сетям. В публикациях всё чаще обсуждается концепция BYOD (bring your own device – принеси собственное устройство). Она предполагает, например, использование собственного планшета или мобильного телефона в служебных/производственных целях. Сторонники концепции уверены, что привычное для человека устройство не потребует большого времени на обучение. Однако подключение к системе автоматизации личного смартфона с неизвестным и неконтролируемым набором ПО представляет серьёзную потенциальную опасность.

Среди угроз, ставших возможными благодаря новым технологиям, можно выделить следующие:

- удалённый доступ к элементам АСУ ТП и нарушение логики работы системы;
- блокировка злоумышленником действий оператора АСУ ТП, подмена информации в интерфейсе оператора;
- включение интеллектуальных элементов инфраструктуры АСУ ТП в состав сетей Ботнет (сети, образуемые взломанными устройствами, функционирующими в целях кибертеррористов/хакеров).

Эксплуатация уязвимостей

Киберпреступники крайне изобретательны в достижении своих целей – эксплуатация уязвимостей в системе для внедрения вредоносного кода или непосредственной атаки, направленной на целостность системы. Вредоносная программа может открывать компьютерные порты, отключать системы безопасности или атаковать определённые приложения или службы. Последствия всего этого могут быть плачевными.

От утечки конфиденциальных данных...

Вредоносная система под условным названием VPNFilter содержит программный код, перекликающийся с версиями вредоносного ПО BlackEnergy, ответственного за несколько крупномасштабных атак, направленных на устройства на Украине. В группе риска – сетевое оборудование Linksys, MikroTik, NETGEAR и TP-Link для малого и домашнего офиса (SOHO), а также устройства сетевого хранения QNAP (NAS). Компоненты модульной вредоносной программы VPNFilter осуществляют кражу учётных данных и мониторинг распространённого протокола SCADA-систем Modbus. Программа VPNFilter способна сделать заражённое устройство полностью непригодным для использования, таким образом заблокировав доступ в Интернет для сотен тысяч жертв во всём мире.

...до промышленных диверсий...

Что же касается специфической опасности для промышленных систем управления, то здесь можно привести в пример печально известный червь Stuxnet, перехватывавший и модифицировавший трафик между контроллерами SIMATIC S7 производства SIEMENS и SCADA-системой SIMATIC WinCC. При помощи Stuxnet, эксплуатирующего уязвимости в ОС Windows и человеческий фактор (Stuxnet распространялся посредством USB-флэш-накопителей), было совершено нападение на объекты ядерной промышленности в Иране. Атака имела итогом физическое уничтожение 1368 центрифуг на заводе по обогащению урана в районе города Натенз и утечку радиоактивного гексафторида урана. Вот как прокомментировал ситуацию Евгений Касперский: «Stuxnet не крадёт деньги, не шлёт спам и не ворует конфиденциальную информацию, «зловред» создан, чтобы контролировать производственные процессы и управлять огромными производственными мощностями. В недалёком прошлом мы боролись с киберпреступниками и Интернет-хулиганами, теперь наступает время кибертерроризма, кибероружия и кибервойн».

...и кражи компьютерных ресурсов

Появляются и более экзотические цели вирусных атак на промышленные системы. Например, в феврале 2018 года, по данным Security Week, было обнаружено заражение программой-червём четырёх подключённых к сети серверов на европейском объекте очистки сточных вод. Заражённые серверы работали под управлением Windows XP и программного обеспечения CIMPLICITY SCADA от GE Digital. Этот инцидент явился первой документированной атакой вредоносного ПО для майнинга криптовалюты, поразившей сеть оператора критической инфраструктуры. Червь в процессе своей работы (майнинга криптовалюты Monero) отбирал значительную долю вычислительной мощности серверов, что вызвало резкое замедление работы ПО мониторинга и управления физическими процессами в реальном времени на объектах водоочистки. Специалисты выяснили, что для незаметной работы и максимального увеличения своей производительности вредоносная программа отключила штатные инструменты безопасности. В отличие от заражения с целью вымогательства этот вид атаки вредоносного ПО

представляет собой новую угрозу, поскольку работает в скрытом режиме и имеет целью оставаться незамеченным в течение длительного времени. Несмотря на то что вредоносная программа смогла заразить HMI-серверы оператора критически важной инфраструктуры, атака, вероятно, не была специально нацелена на объект водоканала.

По данным «Лаборатории Касперского», за прошедшее время число компьютеров, на которых были предотвращены заражения «майнинговыми» вредоносными программами, резко возросло.

Непростая задача

Не только пользовательские, но и автоматизированные промышленные объекты с каждым годом всё больше заражаются распространяемыми вредоносными программами, и количество случайных или намеренных атак на объекты ICS (промышленные системы кибербезопасности) всё увеличивается. Очевидно, обеспечение кибербезопасности, как и любые другие меры защиты, должно носить комплексный характер и требует тщательного анализа всех потенциально слабых мест защищаемой системы. Вследствие этого затраты на кибербезопасность неуклонно растут. Если, по данным Forbes, в 2015 году глобальный рынок кибербезопасности достигал $75 млрд, то в нынешнее время он продолжает активно развиваться и, как ожидается, к 2020 году достигнет более $170 млрд.

Компоненты «на переднем фронте», нуждающиеся в самом пристальном внимании, – это оконечные сетевые устройства: компьютеры, маршрутизаторы, облачная среда. К наиболее распространённым технологиям, используемым для защиты перечисленных компонентов, относятся межсетевые экраны, фильтрация DNS, защита от вредоносного ПО при помощи антивирусов. Современные ПЛК, сетевые маршрутизаторы, сетевые видеокамеры, интеллектуальные датчики имеют встроенную собственную операционную систему и простейшую систему защиты (проверка пароля, «белые» и «чёрные» списки IP-адресов и т.п.). Как следствие, всё это оборудование может быть некорректно сконфигурировано. Например, нередки случаи, когда злоумышленники получали доступ к ПЛК после ввода пароля, по умолчанию установленного производителем. Таким образом, важным аспектом обеспечения безопасности является и корпоративная культура, предполагающая строгое соблюдение персоналом комплекса правил работы с компьютерным оборудованием и программным обеспечением.

SCADA – не исключение

Как уже было сказано, защита от киберугроз – решение комплексное. Применительно к SCADA это означает, что задуматься о безопасности надо на этапе выбора, проектирования и развёртывания системы. В идеале она не должна иметь слабых мест, позволяющих:

- несанкционированно изменять конфигурацию системы;
- нарушить ваш контроль над системой;
- получить доступ к базам данных системы с возможностью их изменения;
- получить доступ к системной информации (перехват системного трафика).

Способы защиты на примере ПО ICONICS

Компания ICONICS, которая является одним из мировых лидеров в области разработки программного обеспечения для АСУ ТП и АСУП уже свыше 30 лет, очень серьёзно относится к вопросу кибербезопасности и защиты [1]. На уровне SCADA-систем ICONICS GENESIS32 и GENESIS64 защита осуществляется несколькими способами – обфускацией (запутыванием) исходных кодов, взаимодействием с центрами реагирования на инциденты (ICS-Cert, Kaspersky Lab ICS CERT) и последующим выпуском рекомендаций по снижению рисков [2]. Встроенный в SCADA ICONICS сервер безопасности Security Server разграничивает доступ к управлению по ролям зарегистрированных пользователей и групп с возможностью интеграции с Active Directory. Сервер безопасности ICONICS можно настраивать как для действий в приложениях, так и для тревог, файлов, узлов/станций, активов, отчётов, транзакций и взаимодействий с мобильными устройствами. При этом используются алгоритмы шифрования RSA (512- и 1024-битное шифрование) и RC2 (40- и 128-битное шифрование). Для повышения надёжности работы с сервисами служб ICONICS и шлюзами данных (OPC) можно включать/отключать интерфейсы WCF, REST, OPC UA и целого списка Point Manager (рис. 1). При необходимости веб-взаимодействий и доступа к опубликованным данным с мо-

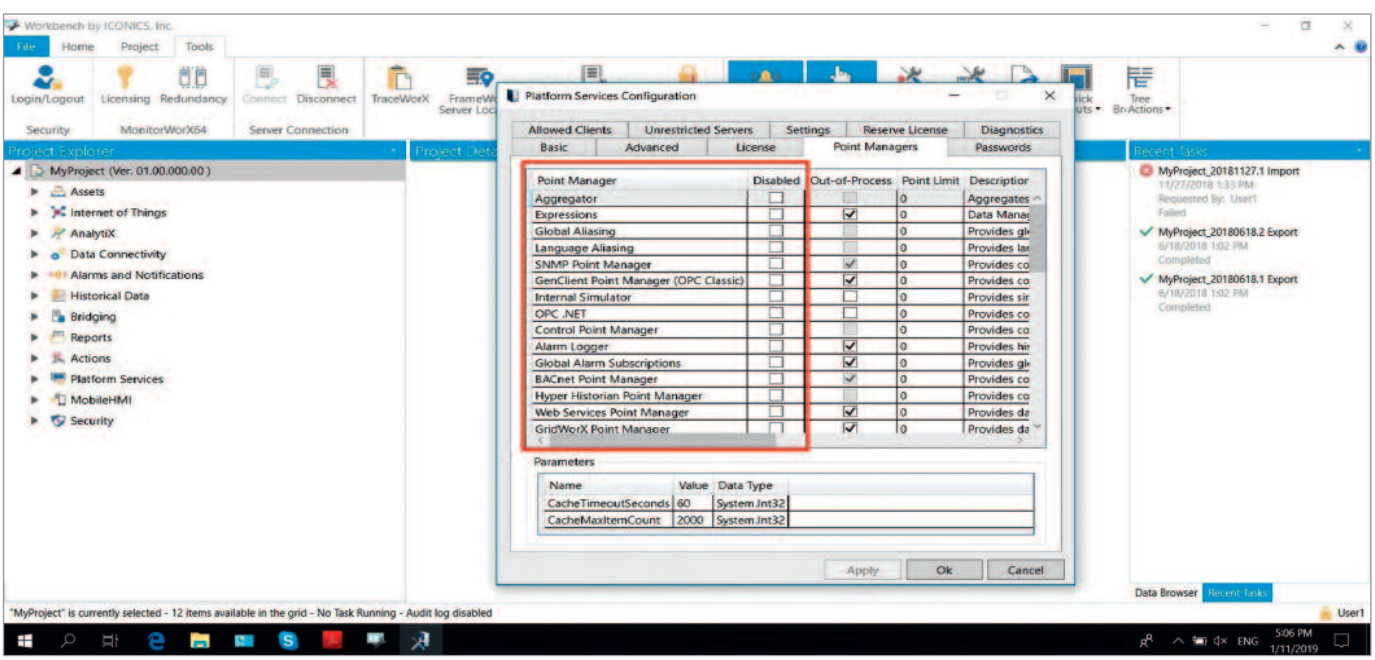

Рис. 1. Конфигурация сервисов ICONICS

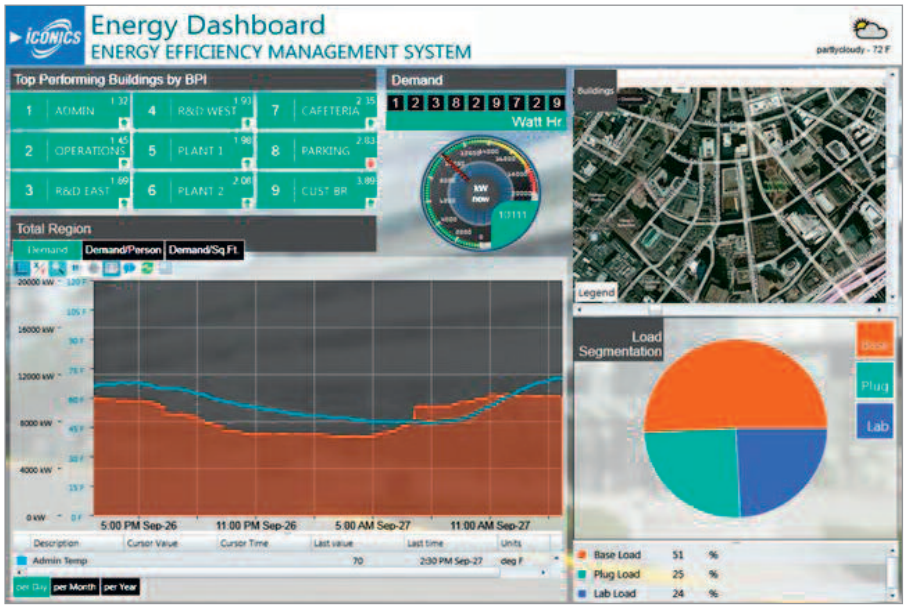

Рис. 2. Данные по энергопотреблению и работе оборудования в Energy Dashboard

бильных устройств используется HTTPS (безопасный протокол HTTP с добавлением криптографического протокола TLS) или SSL-шифрование.

При подключении программных модулей ICONICS к работе с сервисами современных технологий (для создания цифровых близнецов, при работе с дополненной и смешанной реальностью, в облачных вычислениях и машинном обучении) используются только надёжные архитектуры. Например, 23 апреля 2018 года в Ганновере компания ICONICS совместно с Microsoft продемонстрировала интерфейс дополненной реальности на основе устройства HoloLens от Microsoft. Была также продемонстрирована система Facility AnalytiX®, предоставляющая инструмент для предиктивного анализа, обнаружения неисправностей и повышения эффективности обслуживания инженерных систем. Обслуживающему персоналу посредством шлема дополненной реальности может быть передана дополнительная полезная информация: руководства по ремонту, видео и информация из чатов. Всё это ненавязчиво накладывается на поле зрения работника. В данном случае ПО ICONICS тесно взаимодействует с облачными сервисами Microsoft через Azure IoT Hub с двунаправленным транспортным протоколом AMQP, который ранее использовался в банковском секторе и считается одним из самых безопасных в мире благодаря уровню шифрования.

Ещё один пример использования современных технологий с ПО ICONICS – решение цифровых двойников для умных пространств, которое было анонсировано на Всемирном IoT-конгрессе в Испании (IoT Solutions World Congress 16–18 октября 2018 года). Безопасность такого решения начинается с проверки на уровне взаимодействия с оборудованием: программа ICONICS IoTWorX устанавливается на аппаратный IoT-шлюз с использованием криптопроцессора спецификации TPM (Trusted Platform Module), который хранит RSA-ключи шифрования, привязанные к определённой системе аппаратной конфигурации. Собранные в IoTWorX данные по энергопотреблению и работе оборудования инженерных систем автоматизации (рис. 2) передаются на платформу с машинным обучением Microsoft Azure Machine Learning по AMQP с TLS-шифрованием и x.509-сертификатами соединения. Результаты аналитики и виртуального моделирования Microsoft Azure Digital Twins выдаются на программные панели ICONICS Smart Spaces, которые наглядно демонстрируют варианты оптимизации для эффективного управления оборудованием, энергоэффективностью и пространствами контролируемых помещений.

В нашей стране представленными технологиями интересуются, но ещё не очень доверяют и внедряют на отечественных промышленных объектах. Поэтому особый акцент по кибербезопасности в России ICONICS делает на проверке уровня локальных узлов АСУ ТП и межсетевого взаимодействия в распределённых архитектурах. В 2017 году компания ICONICS прошла сертификацию с решением «Лаборатории Касперского» по кибербезопасности АСУ ТП – Kaspersky Industrial Cyber Security (KICS). В процессе сертификации было проведено 19 тестов по защите различных уровней промышленной инфраструктуры, работающих на базе SCADA-пакета ICONICS GENESIS64 10.95, сервера-хранилища с возможностью высокоскоростной обработки данных ICONICS HyperHistorian 10.95, мобильных приложений ICONICS MobileHMI 10.95 и сервера аналитики ICONICS AnalytiX 10.95. В рамках тестов была проверена защита рабочих станций, серверов и ПЛК в промышленной сети от угроз, а также проведён пассивный мониторинг сетевого трафика и соединений промышленной сети. Полученный в результате сертификат предоставляет возможность применения средств защиты KICS на объектах промышленной и критической инфраструктуры, построенных на базе решений ICONICS.

Рекомендации ICONICS по защите системы АСУ ТП с сервером безопасности

- При установке SCADA-системы ICONICS GENESIS64 необходимо настроить конфигурацию сервера безопасности ICONICS Security Server и отменить доступ неавторизованным операторам к настройкам сервера Security.
- Настройте автоматический выход из системы для пользователей, предотвращая неавторизованный доступ к системе.
- Не запускайте сервисы, в работе которых нет необходимости в вашем проекте. Например, при использовании центрального FrameWorX-сервера отключите локальные FrameWorX-сервисы. Также рекомендуется отключать неиспользуемые Point Managers (рис. 1) и остановить их службы.
- Отключите интерфейс OPC UA, если вы не используете сторонние (не от ICONICS) OPC UA-клиенты.
- При использовании сторонних OPC UA-клиентов настройте безопасность через OPC UA Configuration Tool.
- Если в проекте вы используете скрипты с доступом на запись, подключите отчётность по работе скрипта в сервер событий ICONICS GenEvent для трассировки и отчётности всех выполняющихся операций на запись.
- Если вы работаете с ICONICS Security в режиме «Базы данных» с интеграцией Active Directory, используйте бинарный TCP или HTTPS в качестве протокола работы FrameWorX (не HTTP).
- При настройке межсетевого взаимодействия измените порт GenBroker, настроенный по умолчанию.

- Используйте SCADA совместно с протестированными решениями кибербезопасности.

Kaspersky Industrial Cyber Security

Максимальной безопасности без привлечения средств сторонних разработчиков, например, антивирусного ПО, сетевых экранов и т.п., добиться нельзя. Из числа отечественных инициатив стоит выделить набор технологий и сервисов, созданных для защиты различных уровней промышленной инфраструктуры и других элементов предприятия, в том числе серверов SCADA, операторских панелей, инженерных рабочих станций, ПЛК, сетевых соединений и даже самих инженеров – Kaspersky Industrial CyberSecurity (KICS). Это ПО «Лаборатории Касперского» является универсальным и применимо для защиты промышленных предприятий практически любых отраслей. KICS состоит из набора компонентов, ориентированных на решение определённых задач.

- KICS for Nodes (KICS для узлов). Этот компонент предназначен для установки на конечных станциях под управлением ОС Windows: рабочие станции операторов, инженерного персонала, серверы и т.д. Он проводит контроль запуска приложений с использованием «белого» списка разрешённых приложений, контроль подключения к рабочей станции внешних накопителей, антивирусную защиту и сканирование в реальном времени, используя «белый» список доступа к общим ресурсам. Для гарантированной работы компонента решение протестировано на совместимость с популярными SCADA-системами;
- KICS for Networks (KICS для сетей). Данный компонент является анализатором трафика промышленных сетей. В отличие от предыдущего он не оказывает влияния на систему и не имеет механизмов вмешательства в работу технологических процессов;
- Kaspersky Security Center (KSC). Это инструмент администрирования, позволяющий централизованно и удобно управлять указанными компонентами.

Как и все комплексные антивирусные решения, KICS требует квалифицированной установки, настройки и тестирования на совместимость с используемым рабочим ПО.

Рекомендации «Лаборатории Касперского»

В числе не требующих глубоких изменений простейших правил безопасности для промышленных систем «Лаборатория Касперского» рекомендует [3]:

- защитить все узлы промышленной сети от вредоносных атак при помощи средств антивирусной защиты;
- настроить правила сетевых экранов на границе технологической сети;
- настроить защиту от спамовых и фишинговых рассылок на границе и внутри корпоративной сети;
- настроить антивирусную защиту на периметре сети организации и контроль обращения к вредоносным и потенциально опасным интернет-ресурсам;
- провести аудит использования почты внутри технологической сети;
- провести аудит использования папок общего доступа внутри технологической сети;
- провести аудит использования сторонних средств удалённого администрирования внутри технологической сети, таких, как VNC, RDP, TeamViewer RMS/Remote Utilities. Удалить все средства удалённого администрирования, не обусловленные производственной необходимостью;
- отключить средства удалённого администрирования, поставляемые вместе с ПО АСУ ТП (обратитесь к документации на соответствующее ПО за детальными инструкциями), если в их использовании нет производственной необходимости;
- провести аудит использования прочего ПО в технологической сети, которое существенно увеличивает поверхность атаки систем АСУ. В случае если использование этого ПО не обусловлено технологической необходимостью, деинсталлировать его. Особое внимание уделить следующим типам ПО:
  - выключить Windows Script Host, если его запуск не требуется для работы ПО АСУ ТП и не обусловлено другой производственной необходимостью;
  - при возможности ограничить использование привилегий SeDebugPrivilege для локальных администраторов систем промышленной сети предприятия при помощи групповых политик домена Windows (может требоваться для работы некоторого ПО, например, MS SQL Server – обратитесь к документации производителей соответствующих систем).

Выводы

Промышленная революция с концепцией Индустрии 4.0 предполагает использование современных технологий в системах автоматизации промышленных объектов с обязательным подключением к сети. С одной стороны, использование такой концепции помогает выйти на более современный уровень производства, повышая качество управления и обслуживания систем и оборудования, снижая энергозатраты, простои и влияние человеческого фактора.

С другой стороны, в таких системах повышается потенциальная угроза предоставления несанкционированного доступа злоумышленникам с перехватом управления промышленными системами автоматизации. Поэтому к выбору системы для управления АСУ ТП нужно относиться серьёзно, предпочитая производителей с многолетним опытом работы в системах автоматизации, непрерывно повышающих безопасность своих решений через алгоритмы шифрования, тестирования, с сертификацией и современными системами кибербезопасности. В статье были представлены современные технологии, применяемые в рамках четвёртой индустриальной революции, даны примеры их использования и перечислены основные киберугрозы, которые можно ожидать в рамках этих технологий. Даны рекомендации по защите SCADA-уровня от одного из лидеров рынка программных решений промышленной автоматизации и управления инженерными системами зданий – компании ICONICS, а также список основных правил по безопасности от российской компании «Лаборатория Касперского». ●

Литература

1. Highly Secure HMI SCADA and Automation Systems: ICONICS WhitePaper [Электронный ресурс] // Режим доступа : https://iconics.com/Site/Documents/WhitePapers/Highly-Secure-HMI-SCADA-and-Automation-Systems.aspx.
2. Security Updates [Электронный ресурс] // Режим доступа : https://iconics.com/certs.
3. Ландшафт угроз для систем промышленной автоматизации: первое полугодие 2018 [Электронный ресурс] // Режим доступа : https://ics-cert.kaspersky.ru/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/.

Телефон: (495) 234-0636
E-mail: info@prosoft.ru

Fastwel

-40°C / +85°C

РОССИЙСКАЯ ЭЛЕКТРОНИКА ДЛЯ ОТВЕТСТВЕННЫХ ПРИМЕНЕНИЙ

STACKABLE StackPC COMPUTERS

StackPC: гибкость, надёжность, универсальность

- Разработано и произведено в РФ
- Долговременная доступность
- Выделенная техническая поддержка

ProSoft®

WWW.PROSOFT.RU

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

МОСКВА
(495) 234-0636
info@prosoft.ru

САНКТ-ПЕТЕРБУРГ
(812) 448-0444
info@spb.prosoft.ru

ЕКАТЕРИНБУРГ
(343) 356-5111
info@prosoftsystems.ru