Методология безопасности АСУ ТП

в контексте «Интернета вещей»

Александр БУРЦЕВ,
директор департамента АСУ ТП,
ЗАО «НТЦ «Станкоинформзащита»

На современном этапе развития промышленности автоматизированные системы управления технологическими процессами (АСУ ТП) являются неотъемлемой составляющей любого производства. Хотя еще не так давно основным типом систем управления были системы автоматического регулирования (САР), в которых объектами управления были отдельные параметры, установки, агрегаты.

Кроме того, АСУ ТП постепенно приближаются к вопросам жизнедеятельности человека, отходя от первоначальной направленности исключительно на технологические процессы. Такие системы уже можно встретить в автоматизации транспорта, инфраструктурных объектов, коммерческих жилых помещений. Несомненно, вид и составные части АСУ при этом меняются, трансформируясь под требования объекта автоматизации.

Традиционная схема АСУ ТП представлена на рисунке.

В целом концепция любой АСУ сводится к получению и обработке информации, предоставлению необходимых данных пользователю и осуществлению управления на основе полученной информации. Если рассмотреть данное определение в контексте жизнедеятельности человека, то нетрудно заметить прямые аналогии с концепцией «умного дома».

В современном мире все больше привычных устройств включают в себя отдельные элементы АСУ ТП. Системы освещения, кондиционирования и отопления, множество бытовых приборов создаются с возможностью интеллектуального удаленного управления. Все это описывается концепцией «Интернет вещей».

Уже сейчас на рынке представлены такие интеллектуальные устройства с возможностью подключения к сети Интернет, как кухонная и бытовая техника, системы контроля и безопасности, управления климатом в помещении, системы для фитнеса, системы помощи человеку, игрушки и многие другие.

По прогнозу BI Intelligence [1, 2], количество «умных» устройств к 2018 г. возрастет с 2 до 9 млрд. Увеличение количества таких устройств в расчете на одного человека ведет к необходимости автоматизации контроля и управления ими.

Исходя из прогноза можно сделать вывод, что в ближайшие пять-десять лет количество информации, поступающей от всех интеллектуальных устройств, превысит возможности обработки человеком, что повлечет за собой повсеместное распространение домашних интеллектуальных систем управления, по функциональности эквивалентным контроллерам АСУ ТП.

Такие системы используют различные, не всегда совместимые друг с другом технологии и протоколы для связи интеллектуальных устройств, входящих в их состав.

Не секрет, что вопросы информационной безопасности промышленных АСУ ТП стали беспокоить специалистов не так давно. Обусловлено это в первую очередь тем, что в последнее время публичные сети связи (в частности, Интернет и локальные сети предприятий) разрослись до таких масштабов, что стали тесно соприкасаться с сетями АСУ ТП, а иногда даже и пересекаться с ними. Исходя из концепций «умный дом» и «Интернет вещей» их системы управления изначально подключены к публичным сетям, а для некоторых устройств работа в Сети будет основным способом связи. Поэтому вопросы информационной безопасности интеллектуальных устройств и их сетей связи должны рассматриваться уже сейчас. На данный момент в «Интернете вещей» пока не сложились четкие требования к основным элементам, таким как устройства, каналы связи и контроллеры, еще не приняты стандарты, регламентирующие разработку и сопряжение таких

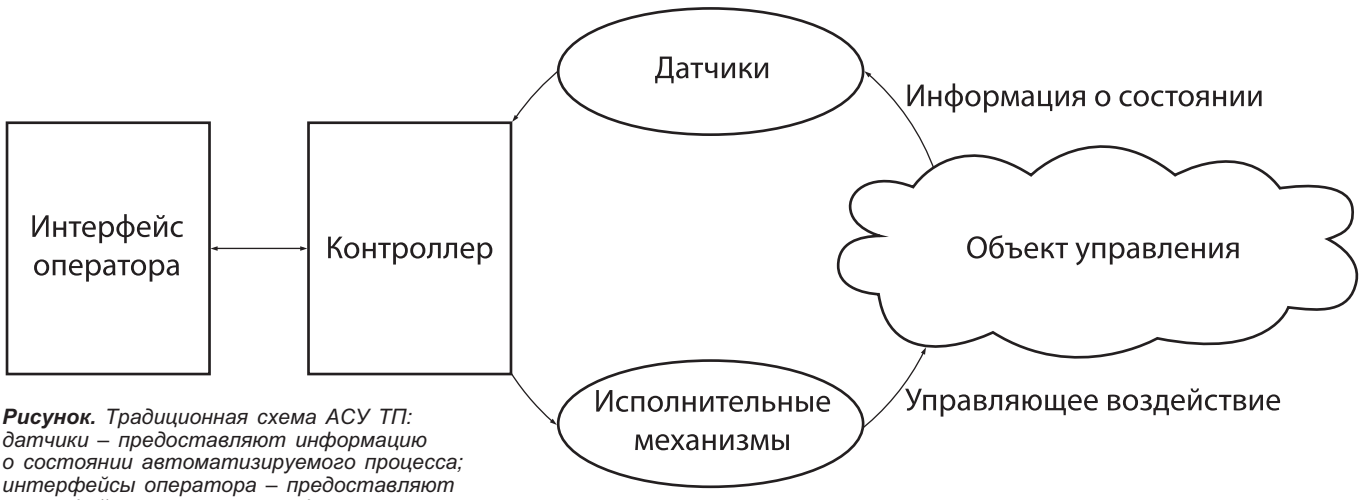

Рисунок. *Традиционная схема АСУ ТП: датчики – предоставляют информацию о состоянии автоматизируемого процесса; интерфейсы оператора – предоставляют интерфейс управления и информацию о текущем состоянии системы оператору; контроллеры – выполняют анализ принятой от датчиков информации и с учетом решений оператора определяют воздействие на автоматизируемый процесс; исполнительные механизмы – осуществляют заданное воздействие на автоматизируемый процесс*

устройств. Сейчас на рынке представлен широкий спектр систем связи и реализующего их оборудования, существует множество протоколов и способов интеграции различных устройств в единую систему «умного дома».

По итогам исследований безопасности широкого спектра промышленных программируемых логических контроллеров (ПЛК), проведенных специалистами нашей компании, можно сделать вывод, что ключевая проблема современных технологий АСУ ТП – отсутствие механизмов контроля достоверности информации. Выражается это, в частности, в отсутствии механизмов взаимной аутентификации устройств между собой, что позволяет злоумышленнику представляться доверенным устройством и оказывать влияние на систему и объект управления.

Заметим, что концепция «Интернета вещей» в первую очередь подразумевает взаимодействие устройств между собой, но вот вопросы взаимного доверия большинством производителей пока не рассматриваются.

Проанализируем основные проблемы безопасности информации в промышленных АСУ ТП и их возможное отражение в рамках концепции «умного дома».

Основными векторами атак на промышленные АСУ ТП являются следующие.

Отказ в обслуживании устройств путем периодической отправки специализированных команд

Большинство интеллектуальных устройств, как промышленных, так и бытовых, имеют весьма ограниченные вычислительные ресурсы, поэтому отправка специально подготовленных команд, требующих дополнительных вычислений, может привести к отказу в обслуживании.

Еще одной возможностью атаки на отказ в обслуживании является периодическая отправка специализированных команд, например перезагрузки, приводящих к кратковременной приостановке работы устройства. Для «Интернета вещей» указанные атаки могут быть реализованы в том случае, если в устройстве отсутствуют механизмы контроля достоверности принимаемой информации.

Отказ в обслуживании устройств с использованием уязвимостей встроенного ПО

В современных интеллектуальных устройствах широко используются специализированные компьютеры, основанные на различных операционных системах (ОС). Кроме того, в них установлено специализированное ПО (СПО), реализующее функционал устройства. При этом, как и любая достаточно сложная система, и ОС, и СПО имеют ошибки, которые могут приводить к появлению уязвимостей в сетевом коде.

Как показывает практика, количество ошибок обратно

> Концепция «Интернета вещей» в первую очередь подразумевает взаимодействие устройств между собой.

пропорционально вниманию к ПО со стороны исследователей безопасности и степени внутреннего тестирования, поэтому уязвимостей в ПО общего назначения (например, браузерах) существенно меньше, чем во встроенном ПО интеллектуальных устройств.

По нашим данным, в промышленных ПЛК больше всего уязвимостей содержится в обработке специализированных протоколов, при этом основная проблема – обработка ситуаций, выходящих за рамки их регулярного применения.

Изменение переменных текущего состояния системы с использованием промышленных протоколов связи

В АСУ ТП устройства предоставляют информацию о состоянии объекта автоматизации в виде значений переменных (тегов), в большинстве случаев достоверность полученной информации ничем не подтверждается. Многие контроллеры предоставляют специализированные команды по изменению как полученной информации, так и внутреннего состояния (как правило, в целях отладки программ управления на устройстве). Посредством использования таких команд возможно введение в заблуждение программы управления контроллера с последующей генерацией некорректных команд управления.

В «умном доме» нарушение целостности информации о состоянии системы может быть использовано для срыва функций управления, что может привести к нарушению таких функций, как энерго- и теплосбережение, создание комфортных климатических условий и т. п.

Внедрение вредоносного кода в программы управления

Одной из интересных особенностей большинства промышленных ПЛК является возможность дистанционного изменения программы управления. Это сделано для облегчения исправления ошибок и настройки оборудования, так как в общем случае контроллеры могут быть установлены на территории предприятия на существенном удалении друг от друга. И хотя некоторые производители реализуют программные (пароли) либо аппаратные (переключатели) ключи, блокирующие возможность изменения программ управления, существует возможность обойти эти механизмы.

> В промышленных ПЛК больше всего уязвимостей содержится в обработке специализированных протоколов.

Используя внедренный в программу управления код, можно оказывать воздействие на всю логику контроллера, тем самым производя любые воздействия на объект управления.

Несмотря на то что сегодня специализированные ПЛК в системах управления «умных домов» практически не используются, в дальнейшем, по мере развития данных систем, для потенциальных злоумышленников открываются широчайшие возможности.

Внедрение вредоносного кода во встроенное ПО устройства

Как уже было сказано, большинство устройств управления представляет собой специализированный компьютер со своими ОС и ПО. Для упрощения исправления ошибок производители предусматривают возможность дистанционного обновления встроенного ПО, при этом лишь немногие реализуют достаточно эффективную систему контроля достоверности таких обновлений, например с использованием цифровых подписей. Для некоторых устройств проверку цифровых подписей можно обойти, используя существующие уязвимости.

Внедрение кода на уровне ОС значительно расширяет возможности злоумышленника, например по доступу к внутренним сетям связи и контролю над всем оборудованием.

Как показывает практика, многие интеллектуальные устройства уязвимы к внедрению кода во встроенное ПО [3, 4].

Таким образом, можно сделать вывод, что большинство проблем, присущих современным промышленным АСУ ТП, будут присутствовать и у домашних интеллектуальных систем. Поэтому при разработке систем типа «умный дом» или очередного интеллектуального устройства необходимо иметь в виду основные проблемы безопасности информации таких устройств. В связи с отсутствием единых стандартов в области построения «Интернета вещей» целесообразно применять те наработки и решения, которые реализуют базовые механизмы защиты от основных угроз безопасности. ■

Ссылки

1. *http://www.businessinsider.com/growth-in-the-internet-of-things-2013-10*
2. *http://www.businessinsider.com/growth-in-the-internet-of-things-market-2-2014-2*
3. *http://www.cnet.com/au/news/fridge-caught-sending-spam-emails-in-botnet-attack/*
4. *http://mashable.com/2013/08/02/samsung-smart-tv-hack/*