Андрей ДУХВАЛОВ:
«Мы считаем необходимым создание Национальной тестовой лаборатории по исследованию проблем безопасности АСУ ТП»

Интервью со стратегом по развитию технологий «Лаборатории Касперского»

– Какие угрозы наиболее актуальны для систем управления технологическими процессами?

– Наиболее актуальны угрозы, способные повлиять на доступность программных или аппаратных узлов, задействованных в управлении технологическим процессом. За ними следуют угрозы, направленные на целостность циркулирующей в сети информации. Они могут возникать на уровне самой технологической сети предприятия и соседствующей с ней корпоративной сети либо проникать извне – из Интернета.

Внутренние угрозы в технологической сети, как правило, связаны с несоблюдением административно-технических мер. В первую очередь речь идет о вредоносном ПО, распространяющемся посредством съемных носителей. Угрозы, приходящие в технологическую сеть из корпоративной сети, включают еще и вредоносное ПО, распространяющееся напрямую по внутренней сети – через общие папки, уязвимости сетевых служб и т. д.

Нередки случаи, когда подсистемы АСУ ТП имеют непосредственный выход в Интернет без использования дополнительных средств защиты – якобы для повышения удобства удаленного управления либо просто по недосмотру. При этом могут использоваться заданные по умолчанию логин и пароль администратора. К сожалению, такие вопиющие случаи не редкость.

– «Лаборатория Касперского» разрабатывает систему обеспечения безопасности АСУ ТП на основе безопасной операционной системы. Какого рода угрозы сможет снять такая система безопасности?

– В основе системы обеспечения безопасности лежит принцип проверки допустимости команд, передаваемых на контроллеры системой управления или АСУ ТП. Это позволяет оградить контроллеры и оборудование, которое находится под их управлением, от неправомерных команд, способных заставить их работать в нештатном режиме. Для системы защиты не важно, что послужило причиной возникновения таких команд: недостатки проектирования, действия оператора, вирусная активность или хакерская атака. В любом случае система безопасности не допустит их исполнения.

Сегодня активно применяются разнообразные методы и средства защиты объектов, где используются АСУ ТП, – физическая охрана периметра, видеонаблюдение, контроль доступа и др. Используются и профилактические меры: обучение персонала, разработка регламентов и т. д. Существующие меры обеспечения безопасности необходимо расширять в направлении защиты от информационных угроз. Именно таким «расширением» и является наша система.

– Чем обусловлена необходимость разработки безопасной операционной системы полностью «с нуля»?

– По сути, в АСУ ТП применяются операционные системы общего назначения: в основном Windows разных версий, иногда Linux-подобные ОС. Особое место занимают проприетарные ОС, применяемые в промышленных программируемых контроллерах. Все они в той или иной степени содержат уязвимости. Об этом говорят многочисленные исследования, например компаний Digital Bond или Positive Technologies, результаты систематизации уязвимостей АСУ ТП, в частности, выполненные организацией US ICS CERT. Накопленные факты свидетельствуют о том, что используемым сейчас в АСУ ТП программным средствам в целом и операционным системам в частности доверять нельзя.

Эти соображения и привели нас к решению создать собственную ОС. Простую, возможно, с ограниченной функциональностью, но, главное, надежную и безопасную.

– Каковы перспективы сотрудничества «Лаборатории Касперского» с производителями аппаратных платформ? Ведь необходимо гарантировать поддержку новой ОС с их стороны?

– Действительно, какова бы ни была степень доверия к операционной системе, ее недостаточно, чтобы обеспечить доверие к решению в целом.

Мы взаимодействуем с довольно большим числом производителей аппаратных платформ, как общего назначения, так и в области управления технологическими процессами, в целях создания программно-аппаратного комплекса обеспечения безопасности АСУ ТП.

Более того, мы предполагаем привлечь к сотрудничеству широкий круг партнеров, занимающихся производством «железа», системной интеграцией, поставками промышленного оборудования и софта, научными разработками и др.

Мы считаем вполне разумным создание консорциума производителей решений безопасности для АСУ ТП.

Также хотелось бы обратить особое внимание на необходимость создания Национальной тестовой лаборатории по исследованию проблем информационной безопасности программных и аппаратных средств АСУ ТП. ■