Виталий ЛЮТИКОВ: «Вопросы защиты АСУ должны решаться на начальном этапе создания системы»

Интервью с начальником управления Федеральной службы по техническому и экспортному контролю

– Каковы, на ваш взгляд, причины обострения интереса к вопросам защиты АСУ ТП в последнее время? Почему именно теперь этой теме стало уделяться особое внимание на государственном уровне?

– Актуальность темы обусловлена, с одной стороны, широким внедрением информационных, в том числе интернет-технологий в системы управления технологическими процессами, а с другой – повышением интереса злоумышленников к такого рода системам. Кто эти злоумышленники? Это могут быть и частные лица, действующие из «спортивного интереса», и иностранные государства, пытающиеся прощупать состояние систем безопасности критически важных объектов, и преступные сообщества. Но в любом случае последствия постороннего вмешательства в работу АСУ ТП могут быть самые плачевные, вплоть до серьезного ущерба экономике страны и гибели людей.

В СМИ широко освещались инциденты, связанные с появлением «червя» Stuxnet и его собратьев (Duqu, Flame, Gauss). Такие инциденты дают основание всерьез говорить об угрозе кибервойн. Некоторые государства рассматривают информационное пространство как особое поле боя (наряду с другими полями – воздухом, землей, водой, космосом), в ряде стран создаются кибервойска. Это не может не вызывать озабоченности.

– В чем состоит специфика задач защиты АСУ ТП? Чем она обусловлена?

– Первая особенность систем управления технологическими процессами – это во многих случаях их специфичность для управляемого объекта или процесса. Вторая особенность заключается в том, что такие системы, как правило, работают в режиме реального или близком к реальному времени. Даже незначительный сбой в системе может привести к лавинообразному нарушению работы объекта. Решить задачу защиты системы реального времени на этапе эксплуатации очень трудно, практически невозможно. Поэтому система защиты должна внедряться в систему управления на этапе создания.

Еще одна особенность – применяемые технические средства и информационные технологии. Это средства и технологии промышленного класса с длительными сроками службы. Обновления для них, устранения ошибок, новые версии выходят редко (сравнительно с общедоступными технологиями).

Наконец, большинство систем управления поставляются иностранными производителями. Регламенты сервисного обслуживания и ремонта систем определяются производителями (поставщиками) этих систем управления. Нередко поставщик требует наличия канала удаленного управления системой. И подчас организация, эксплуатирующая АСУ ТП, даже не знает, какие действия в системе выполняет иностранный поставщик. Некоторые производители, осуществляющие сервисное (гарантийное) обслуживание, работают с выездом на объект, но не дают специалистам заказчика доступа к своему оборудованию и ПО. Конечно, это негативно сказывается на состоянии защищенности систем управления.

– Кто, с вашей точки зрения, должен отвечать за безопасность АСУ ТП критически важных объектов? Это в первую очередь государство в лице уполномоченных органов или сами владельцы объектов?

– Мы считаем, что заниматься вопросами обеспечения безопасности критически важных объектов должны все, каждый – на своем участке. Есть уполномоченные федеральные органы исполнительной власти, такие как ФСБ России и ФСТЭК России, они разрабатывают общие требования и общие подходы к обеспечению безопасности АСУ ТП, организуют и осуществляют в соответствии с законодательством контроль защищенности систем управления. Есть отраслевые регуляторы – министерства и другие профильные государственные организации. Их задача – конкретизировать и адаптировать общие требования с учетом отраслевой специфики. Важную роль в выработке отраслевых рекомендаций играют и крупные корпорации, такие, например, как «Газпром» или «Русгидро». У этих организаций создан значительный задел в разработке корпоративных стандартов и политики безопасности АСУ ТП. А дело конкретных субъектов – выполнять эти рекомендации.

– По вашим наблюдениям, признается ли актуальность вопроса защиты АСУ ТП руководителями предприятий?

– Ситуация меняется со временем. Сейчас руководители

начинают уделять все больше внимания вопросам защиты АСУ ТП. Да и общество в целом яснее осознает серьезность проблемы. Два-три года назад вопросам безопасности АСУ ТП посвящались одно-два мероприятия в год, сегодня конференции и форумы по этой теме проводятся почти каждый месяц.

Но в целом направление безопасности АСУ ТП развивается на предприятиях медленнее, чем применяемые в них информационные технологии. В первую очередь это связано с дополнительными расходами на защиту систем управления и квалификацией работников, ответственных за безопасность. В большинстве организаций ответственные специалисты просто не умеют определять потенциальный ущерб от нарушения информационной безопасности и обосновывать перед руководством необходимость внедрения системы информационной безопасности. Для предприятий, у которых приоритет – экономическая выгода, это наиболее серьезная проблема.

> Специалисты, средства защиты информации, нормативная база — основа любой системы безопасности.

Некоторые вузы занялись подготовкой специалистов по безопасности АСУ ТП. По мере возрастания спроса на таких специалистов процесс, я думаю, пойдет активнее. На рынке появляются организации, которые изучают вопросы защиты АСУ ТП, создают у себя профильные направления. Пока таких организаций немного, хотелось бы, чтобы их было больше, тем не менее какую-то часть проблемы они способны закрыть.

> Каждый на своем участке должен обеспечивать безопасность критически важных объектов.

– Достаточно ли сейчас на рынке ресурсов, чтобы обеспечить полноценную защиту АСУ ТП, в том числе компетентных специалистов и технических средств защиты?

– Любая система безопасности, будь то федерального уровня, регионального или объектового, базируется на трех основах: подготовленных специалистах, средствах защиты информации, нормативной базе. По всем трем направлениям мы наблюдаем поступательное движение.

В части нормативной базы заинтересованными органами и организациями ведется работа по реализации «Основных направлений государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации», утвержденных Президентом Российской Федерации в феврале прошлого года.

Что касается сертифицированных средств защиты, которые могли бы применяться в АСУ ТП, то в этой части сегодня необходимо решить ряд проблем, связанных с использованием средств защиты в системах реального времени. Например, система обнаружения вторжений, будучи установленной в систему управления реального времени, может воспринять управляющую команду как атаку и блокировать трафик. Последствие – остановка технологического процесса. Организации, которые эксплуатируют АСУ ТП, пытаются выходить из положения путем перенастройки подобных средств защиты, что не всегда удается. Поэтому при разработке требований к средствам защиты информации мы будем исходить, в частности, из возможностей их использования в АСУ ТП. Однако с учетом уникальности систем управления об этом необходимо задумываться прежде всего заказчику на этапе задания требований и проектирования системы управления.

– Насколько усложняет задачу защиты АСУ ТП тот факт, что многие из подобных систем уникальны, создавались давно и с использованием устаревших языков?

– Проблема безопасности АСУ ТП, созданных 20–30 лет назад, конечно, существует, но она не так драматична, как некоторым кажется. Да, на старую систему невозможно поставить современное средство защиты, но и атаку на нее сформировать непросто. К тому же степень автоматизации в этих системах минимальна.

Гораздо больше беспокоит уровень защищенности новых систем, которые в значительной степени автоматизированы и где применяются современные информационные технологии. Мы настаиваем на том, что вопросы защиты АСУ должны решаться на начальной стадии ее создания, при формировании концепции автоматизации производства. Когда АСУ ТП запущена в эксплуатацию, защитить ее без остановки производственного цикла уже невозможно. Методические документы ФСТЭК России для того и разработаны, чтобы организации их использовали на начальном этапе, при формировании концепции автоматизации и написании ТЗ. При этом должна быть проведена адаптация приведенных в методических документах положений к производственному процессу и автоматизированной системе управления.

Руководитель, придерживающийся такого подхода, будет для управления критическим процессом выбирать систему, в которой требования безопасности уже реализованы на этапе проектирования, и иметь значительно меньше проблем при ее эксплуатации. ■