Система защиты информации (ЗИ) как составная часть АСУ ТП

В статье обосновывается необходимость использования средств информационной безопасности (ИБ) при построении АСУ ТП, описываются методы проектирования таких систем, а также предлагается решение – киберзащищенный программно-технический комплекс.

ОАО «ИнфоТеКС», г. Москва
Компания «ИнСАТ», г. Москва

Большинство вновь разрабатываемых, проектируемых информационных и управляющих систем призваны обеспечить рост эффективности современного производства, повышение качества выпускаемой продукции, снижение себестоимости, причем с сохранением надежности и безопасности функционирования.

Использование современных инфокоммуникационных технологий – микропроцессорной техники на основе микропроцессоров с самой разной архитектурой, операционных систем (ОС) реального времени, ОС общего назначения, телекоммуникационных технологий и протоколов, несвойственных до последнего времени автоматизированным системам управления (Ethernet, протоколов, базирующихся на стеке протоколов TCP/IP), то есть технологий, изначально разрабатываемых без увязки с обеспечением информационной безопасности, существенно повышает вероятность появления информационных угроз.

Таким образом, к требованиям промышленной безопасности, столь привычным для производственников, добавились менее понятные или совсем непонятные, а часто и не принимаемые требования по информационной безопасности автоматизированных систем управления технологическими процессами.

Между тем стоит отметить, что требования по обеспечению промышленной и информационной безопасности преследуют схожие, если не одинаковые, цели: безопасное функционирование АСУ ТП в штатном режиме в пределах проектных значений. На угрозы и риски, которые могут возникнуть с внедрением информационных технологий без увязки с обеспечением информационной безопасности, также указывает принятая в конце 2016 года «Доктрина информационной безопасности Российской Федерации» [1]. Защита объектов критической информационной инфраструктуры – одна из трех ключевых тем высокоуровневого доктринального политического документа.

Важно, что следующим логичным шагом на пути реализации положений доктрины стало внесение в Государственную Думу пакета проектов нормативно-правовых актов, главным из которых является Законопроект № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации». Данный законопроект был рассмотрен и поддержан депутатами в первом чтении и находится на этапе устранения замечаний при подготовке ко второму чтению. После принятия и вступления в силу федерального закона и пакета подзаконных нормативных актов будет построена законченная логичная вертикаль нормативно-правового регулирования, что является реакцией государства на стремительно меняющийся ландшафт угроз в информационной сфере.

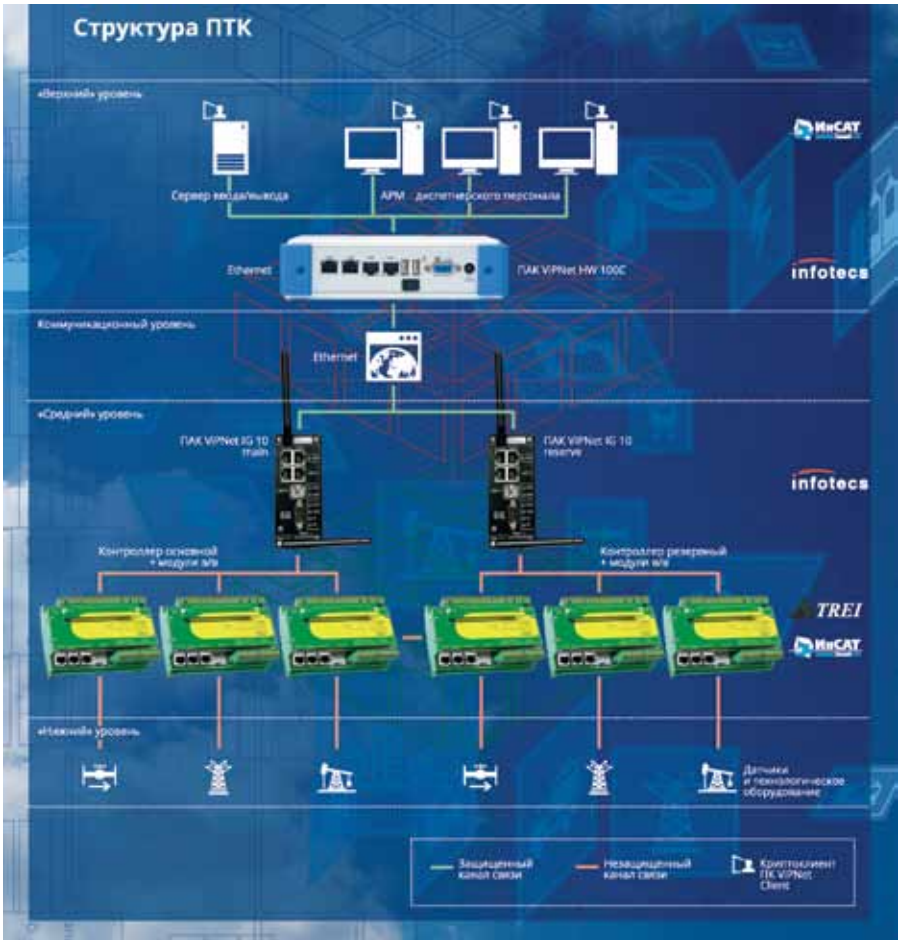
Попробуем разобраться, что же такое информационная безопасность в АСУ ТП и к каким последствиям может привести отсутствие внимания к данной проблеме. Начнем с последнего вопроса. Одним из возможных примеров является случай на Украине, когда из-за хакерской атаки на энергосистему город был лишен всех снабжающих его электроэнергией объектов и у обслуживающих организаций ушел целый день на восстановление полного энергообеспечения. Об убытках, понесенных городом, даже и говорить не стоит.

Другой наглядной иллюстрацией последствий компьютерной атаки на АСУ ТП может служить инцидент, произошедший на одном из сталелитейных производств Германии в 2014 году и расследованный Федеральным управлением по информационной безопасности Германии (BSI). В результате компьютерной атаки на АСУ ТП доменной печи штатное функционирование последней было нарушено, что привело к финансовым убыткам [2].

Защита информации (ЗИ) в АСУ ТП – это в первую очередь правильный подход к проектированию системы, под которой нужно понимать все многообразие управляющих технологическим процессом систем: программно-технические комплексы, распределенные системы управления (РСУ), автоматизированные системы управления технологическими процессами. При этом необходимо учитывать все нормативные требования информационной безопасности и промышленной безопасности (ПБ) применительно к отраслевой специфике, поскольку те или иные промышленные протоколы передачи данных допускают различные варианты всевозможных атак и методов защиты против них. После исследования и систематизации знаний составляются модель угроз и модели нарушителей системы, что позволяет подобрать наиболее правильные методы защиты как внутри периметра, так и вне его. Причем при использовании правильного подхода к проектированию и применению комплекса средств, надежно интегрированных друг с другом, система ЗИ не будет заметна пользователю, а ее функционирование не отразится на быстродействии всей системы. Далее наступает этап разработки, тестирования и сдачи системы заказчику.

Все многообразные средства защиты информации должны входить в любую индустриальную систему как одна из необходимых подсистем – подсистема ЗИ. При реализации подсистемы могут быть задействованы шлюзы безопасности (межсетевые экраны и VPN-шлюзы), интегрированные программно или аппаратно средства криптографической защиты информации, системы обнаружения атак и другие средства ЗИ. Применение отдельных компонентов подобных технологий защиты позволит обеспечить автоматизированные системы необходимым минимумом информационной безопасности, а при совокупном использовании нескольких различных способов защиты можно создать объект с периметром безопасности, который будет достаточно серьезной преградой для сетевого нарушителя.

Технологии ЗИ позволяют обеспечить не только защиту периметра. Во всех системах АСУ ТП используется ролевая система доступа к тем или иным функциям управления объектом, а действия оператора обычно логируются в соответствующем журнале. При внесении в эту функцию двух дополнительных элементов – двухфакторной аутентификации и использования цифровых криптографических подписей – данные могут являться уже не просто данными, а юридически важным документом. Тогда при выяснении обстоятельств того или иного случая будет доподлинно известно, кто стал источником дисбалансирующего управляющего воздействия, которое привело к последующим негативным последствиям.



▲ Структурная схема ПТК с наложенными средствами защиты информации

Руководствуясь необходимостью и востребованностью данного типа систем на современном рынке, компании «ИнСАТ», «ИнфоТеКС» и «ТРЭИ» разработали совместное решение – киберзащищенный программно-технический комплекс (ПТК).

Данное решение сочетает в себе все самые современные наработки в области автоматизированных систем управления и защиты информации. «Железной» составляющей ПТК являются программируемые логические контроллеры серии ТРЭИ-5В-05 с большим числом модулей ввода/вывода, поддерживающих полный перечень сигналов ввода/вывода. Эти контроллеры уже хорошо зарекомендовали себя в качестве средств автоматики с возможностью построения блокировок и защит, а также средств резервирования с широким диапазоном эксплуатации. Кроме того, контроллеры TREI – одни из немногих, имеющих зарубежный сертификат TÜV SIL3.

В качестве среды программирования контроллеров и верхнего уровня используется MasterSCADA – вертикально интегрированная, объектно ориентированная SCADA-система.

В MasterSCADA программирование нижнего и среднего уровней возможно вести на языках стандарта МЭК 61131-3, а одной из отличительных ее особенностей является то, что различные узлы системы (контроллеры, АРМ, серверы) могут обмениваться информацией по общепринятому промышленному

стандарту OPC UA. Кроме того, MasterSCADA – это кроссплатформенный продукт, который поддерживает наиболее популярные операционные системы, в том числе ОС «Эльбрус».

В качестве наложенных средств защиты используются сетевые шлюзы безопасности от компании «ИнфоТеКС» VIPNet Coordinator IG10 и HW100 в индустриальном исполнении, которые организуют виртуальные защищенные сети (VPN) в промышленных системах и сегментируют их на домены.

Разработанное решение универсально и может быть использовано как для создания новых, так и для модернизации существующих систем АСУ ТП в различных отраслях промышленности, в том числе на объектах нефтегазотранспорта, нефтегазодобычи, нефтегазопереработки, химической, металлургической, атомной промышленности, горнодобычи и переработки, машиностроения и на прочих критически важных инфраструктурных объектах. Ведь программно-технический комплекс не имеет жесткой привязки к специфике того или иного объекта, но обладает при этом всеми необходимыми характеристиками ПТК общего назначения. Кроме того, следующий этап партнерства подразумевает возможность использования встроенных в компоненты ПТК средств ЗИ, что еще более повысит надежность данного решения.

Литература

1. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 // «Российская газета» [сайт]: URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 10.04.2017).

2. Robert M. Lee, Michael J. Assante, Tim Conway. ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack [Электронный ресурс] // ICS Defense Use Case (DUC) Dec 30, 2014. URL: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf (дата обращения: 10.04.2017).

В.Г. Карантаев, к. т. н., руководитель направления развития бизнеса компании ОАО «ИнфоТеКС», г. Москва;
тел.: +7 (495) 737-6192,
e-mail: info@ infotecs.ru,
сайт: infotecs.ru

А.М. Подлесный, руководитель отдела продаж программного обеспечения, компания «ИнСАТ», г. Москва,
тел.: +7 (495) 989-2249,
e-mail: info@insat.ru,
сайт: www.insat.ru