Защита АСУ ТП:
текущее состояние и практический опыт

Дмитрий ЯРУШЕВСКИЙ,
CISA, CISM, руководитель отдела кибербезопасности АСУ ТП, ЗАО «ДиалогНаука»

Обеспечение защиты информации (или обеспечение кибербезопасности) в автоматизированных системах управления технологическими процессами (АСУ ТП) – направление для России достаточно новое. Еще несколько лет назад это была проблема, обсуждаемая лишь в узком кругу специалистов и разработчиков АСУ ТП. В наши дни кибербезопасность АСУ ТП превратилась в стремительно развивающееся направление отечественного рынка специализированных средств защиты для промышленных систем и услуг системных интеграторов.

Этому изменению способствовал целый ряд факторов, среди которых можно указать следующие: повышенное внимание регуляторов[1]; развитие автоматизации технологических процессов; увеличение числа доведенных до общественности инцидентов реализации киберугроз на объектах различных отраслей промышленности и энергетики. Например, 245 зарегистрированных инцидентов, по данным только ICS-CERT (The Industrial Control Systems Cyber Emergency Response Team) за, период с сентября 2014 по февраль 2015 г.[2]

Несмотря на быстрое развитие рынка, практического опыта по обеспечению защиты АСУ ТП в России катастрофически мало. Тем не менее даже его достаточно, чтобы выявить некоторые риски системного характера, возникающие при реализации проектов по обеспечению кибербезопасности.

Сложной системой защиты некому управлять

На объектах АСУ ТП зачастую нет специалистов с необходимой квалификацией. У крупного заказчика могут быть специалисты по информационной (или экономической) безопасности корпоративного сегмента и высококвалифицированные специалисты по эксплуатации АСУ ТП, но может не оказаться специалистов по обеспечению кибербезопасности АСУ ТП. При этом защита АСУ ТП – отдельная область информационной безопасности, требующая специальных знаний и компетенции. В результате на объекте заказчика, возможно, просто некому будет передать в эксплуатацию современную систему защиты.

Реактивный режим защиты

Ошибки первого рода (ложноположительные срабатывания) средств защиты информации (СЗИ) могут привести к нарушениям в непрерывности, управляемости и наблюдаемости технологического процесса. Риск таких ошибок, приемлемый и вполне привычный для корпоративных систем, может быть совершенно недопустим для АСУ ТП. Поэтому к режимам предотвращения угроз относятся с особой осторожностью.

Более того, процессы кибербезопасности на предприятиях еще настолько не развиты, что даже при обнаружении системой защиты явного инцидента непонятно, какие действия выполнять дальше.

Приведем пример: система обеспечения информационной безопасности обнаруживает аномальный трафик в технологической сети. Система защиты предполагает, что команды телеуправления отравляются из неизвестного источника (нелегитимный сервер управления). В этой ситуации дежурный диспетчер, с одной стороны, видит сообщение о вероятном инциденте, с другой – наблюдает технологический процесс в штатном режиме. Какие действия он должен предпринять? Кто и на основании чего принимает решения о необходимых действиях? Кто несет ответственность за результаты

---

[1] *Издание в марте 2014 г. приказа № 31 ФСТЭК (Федеральной службы по техническому и экспортному контролю) России «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».*

[2] *ICS-CERT Monitor Newsletter September 2014 – February 2015; US Department of Homeland Security, National Cybersecurity And Communications Integration Center.*

таких действий? Этими вопросами иногда пренебрегают при разработке систем защиты АСУ ТП. Однако же без ответов на них, без выстраивания полного жизненного цикла процесса управления инцидентами такая система не будет эффективной.

У персонала должны быть четкие технологические инструкции, описывающие, что именно и в каких случаях необходимо предпринимать (подобные инструкциям по эксплуатации АСУ ТП). Но, во-первых, для разработки таких инструкций требуются огромный опыт и накопленная база знаний по произошедшим инцидентам и их последствиям, во-вторых, ни одна инструкция не может предугадать развития хорошо продуманной и подготовленной атаки злоумышленника.

Фокус на защите периметра и сетей связи

Для многих объектов подход, ограничивающийся защитой периметра сети, может быть оправдан и эффективен. Но лишь при том условии, что удастся ограничить пересечение сетей АСУ ТП со смежными одной-двумя логическими точками, что сами сети АСУ ТП будут сегментированы, правильно выстроены правила маршрутизации и управления сетевым доступом на телекоммуникационном оборудовании, а все оборудование будет находиться в пределах контролируемой зоны. Однако это не всегда возможно. Ряд промышленных систем строится таким образом, что, например, программируемые логические контроллеры (ПЛК) располагаются на удаленных объектах вне пределов контролируемой зоны. Такие ПЛК (и даже отдельные датчики) могут стать точкой входа для злоумышленника и предоставить ему все возможности для реализации атак на системы верхнего уровня (SCADA – Supervisory Control and Data Acquisition, ERP и даже корпоративные системы, если сети связаны), что продемонстрировали в своих работах эксперты из исследовательской лаборатории[3, 4].

Применение наложенных средств защиты вместо средств АСУ ТП

Системным интеграторам в России хорошо знаком широкий парк традиционных средств и систем защиты, используемых в корпоративных средах. Но иногда применение подобных средств для защиты АСУ ТП может быть избыточным, неэффективным либо вообще негативно влиять на управляемость и наблюдаемость технологического процесса. Кроме того, корпоративные средства защиты информации не предназначены для работы в агрессивных средах и климатических условиях, в которых могут эксплуатироваться средства АСУ ТП. Наконец, большая часть таких систем не предназначена для обеспечения защиты промышленных протоколов связи.

С другой стороны, осуществляемые наложенными средствами меры безопасности зачастую могли бы быть реализованы средствами самой АСУ ТП с минимальными изменениями в конфигурациях. Например, многие SCADA-системы позволяют выполнять мониторинг, в частности систем физической безопасности и управления доступом, регистрацию и сбор событий логического доступа, действий операторов и т. д. Иногда эта функциональность остается незадействованной при создании системы защиты, потому что SCADA входит в зону ответственности подразделений АСУ ТП, в то время как обеспечение кибербезопасности – нет.

Использование возможностей ПЛК

Существует несколько подходов к кибербезопасности, позволяющих минимизировать перечисленные проблемы. Выбор зависит от специфики объекта защиты, технологического процесса и применяемых систем. Одним из таких подходов является использование возможностей ПЛК.

Современные ПЛК по своим функциям и вычислительным ресурсам все больше напоминают промышленные компьютеры. Зарубежные разработчики порой даже отходят от термина Programmable Logical Controller (PLC), используя для своих продуктов понятие Programmable Automation Controller (PAC)[5].

Среди функциональных возможностей ПЛК от различных производителей (как зарубежных, так и отечественных)[6] можно встретить следующие механизмы безопасности:

- аутентификация при удаленном или локальном доступе по протоколам RADIUS (Remote Authentication Dial-In User Service) через внешний сервер;
- VPN/TLS (Virtual Private Network/ Transport Layer Security) с поддержкой шифрования по международным алгоритмам – AES (Advanced Encryption Standard), 3DES (Triple Data Encryption Algorithm) и т. д.;
- подключение к модулю СКУД (система контроля и управления доступом), сбор событий безопасности, сигнализации открытия дверей, пожарной сигнализации и передача событий ИБ внешнему источнику (например, SIEM-системе (Security Information and Event Management);
- межсетевое экранирование.

Реализация и задействование этой функциональности в системе обеспечения кибербезопасности АСУ ТП позволяет:

- минимизировать риски, связанные с реализацией угроз на нижнем уровне АСУ ТП;

[3] *Медведовский Илья. Атака на АСУ ТП: от датчиков до ERP и обратно // Конференция Kaspersky Industrial Security, 2014.*
[4] *Большев Александр, Чербов Глеб. ICSCorsair: как мы взломаем вашу ERP-систему через токовую петлю // Конференция t2'14.*
[5] *Is PLC a Dirty Word Now? / Dan Herbert, technical editor Control Design; Control Design for machine builders, 2012 (http://www.controldesign.com/articles/2012/hebert-is-plc-a-dirty-word-now/).*
[6] *Продукция компаний Phoenix Contact, SoftPLC, ООО «ДЭП» и др.*

- передавать часть функций и ответственности за обеспечение кибербезопасности в руки специалистов по АСУ ТП, что способствует интеграции процессов защиты информации в управление технологическим процессом;
- рассматривать вопросы кибербезопасности при проектировании, создании и модернизации самой АСУ ТП;
- снизить риск возможного негативного влияния и последствий работы средств защиты информации за счет минимизации использования наложенных средств;
- сократить затраты на внедрение и эксплуатацию.

Практический опыт реализации мер безопасности на уровне ПЛК

В ходе работы над одним из проектов по созданию системы обеспечения информационной безопасности АСУ ТП электрораспределительной компании мы столкнулись с задачей по обеспечению целостности потоков данных между удаленными объектами, расположенными в условно неконтролируемой зоне, и центральным диспетчерским пунктом (ЦДП).

Удаленные объекты – это трансформаторные подстанции (ТП), оборудованные контроллером телемеханики. Контроллер осуществляет сбор и передачу в ЦДП телесигнализации и телеинформации. ЦДП передает на этот контроллер команды телеуправления и обновленные конфигурации прошивки контроллера.

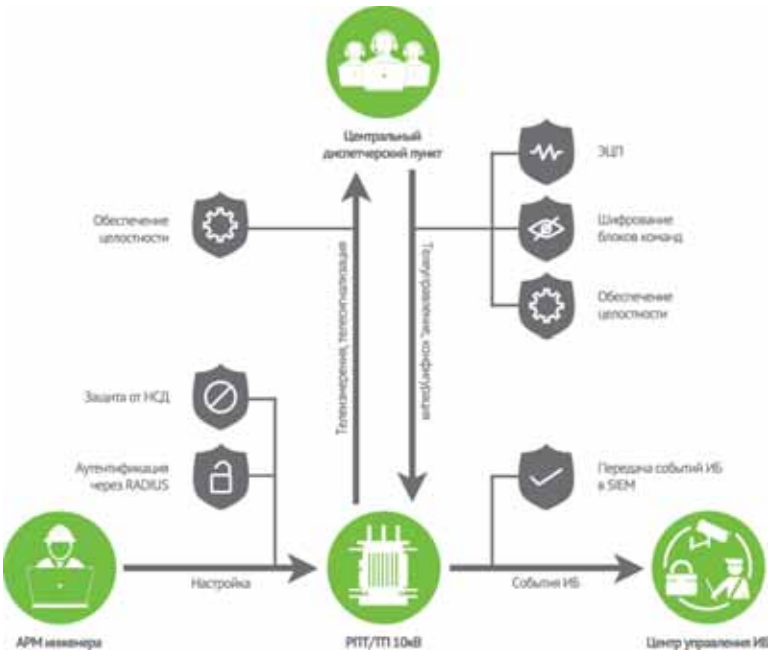
Связь осуществляется по незащищенным линиям (GSM/3G, арендованные каналы).

Перед нами была поставлена следующая задача: обеспечить аутентификацию устройств, централизованную аутентификацию инженеров и подрядчиков, целостность передаваемых данных телемеханики, целостность и авторство передаваемых команд телеуправления и конфигураций оборудования.

При проектировании рассматривались различные варианты решения указанных задач, в том числе за счет использования дополнительных СЗИ, усиления или дополнения мер физической защиты и т. д. Но все эти варианты оказались либо недостаточно эффективными, либо снижающими надежность системы, либо экономически нецелесообразными.

Выбор был сделан в пользу реализации совместного решения с производителем ПЛК и нашим партнером – разработчиком СКЗИ (средства криптографической защиты информации). Суть решения заключается в использовании дополнительного программно-аппаратного криптомодуля, устанавливаемого в корпус контроллера и взаимодействующего по стандартному внутреннему интерфейсу. В комплексе с программным обеспечением ПЛК и системами верхнего уровня такое решение способно обеспечить (см. рисунок):

- аутентификацию по RADIUS при локальном и удаленном подключении;
- шифрование VPN/TLS;
- проверку ЭЦП отдельных блоков команд и конфигураций оборудования, получаемых «сверху»;
- контроль целостности собственных компонентов;
- передачу событий информационной безопасности в систему мониторинга (SIEM).



Все системы АСУ ТП, сами технологические процессы и объекты защиты являются уникальными. Типовых или универсальных решений по обеспечению кибербезопасности, применимых на любом объекте, нет и, скорее всего, не будет. На настоящем этапе развития направления, когда нет даже проверенных путей, один из ключей к эффективной защите АСУ ТП – тщательный выбор и проработка возможных технических решений и взаимодействие всех заинтересованных сторон.

При этом задачу обеспечения кибербезопасности стоит рассматривать как часть более широкой проблемы обеспечения управляемости и непрерывности технологических процессов. Рассмотренный в настоящей статье подход к защите АСУ ТП, с нашей точки зрения, является одним из возможных вариантов эффективной защиты от киберугроз и может успешно применяться в целом ряде российских компаний.

Совместная работа с разработчиками ПЛК и разработчиками криптомодуля сделала возможными тщательные испытания и необходимые доработки решения для максимальной адаптации под нужды и условия заказчика. ■