АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА

ДМИТРИЙ ПОРОДИН
Заместитель директора Департамента информационной безопасности АМТ-ГРУП

В последнее время проблемы безопасности топливно-энергетического комплекса Российской Федерации стали объектом пристального внимания на государственном уровне. Одним из аспектов этого внимания являются вопросы информационной безопасности систем и технологических сетей автоматизированных систем управления технологическими процессами.

Летом этого года принят новый Федеральный закон «О безопасности объектов топливно-энергетического комплекса» (256-ФЗ от 21.07.2011 г.). В целом предметом регулирования данного закона является антитеррористическая защищенность объектов топливно-энергетического комплекса, однако требования по информационной безопасности систем и телекоммуникационных сетей вошли в одну из статей документа. Одновременно с 256-ФЗ был принят Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части обеспечения безопасности объектов топливно-энергетического комплекса» (257-ФЗ от 21.07.2011 г.), который устанавливает уголовную и административную ответственность должностных лиц за нарушение требований безопасности объектов топливно-энергетического комплекса.

Подходы к обеспечению информационной безопасности и технические требования обеспечения безопасности автоматизированных систем управления технологическими процессами регламентируются комплектом документов, выпущенных регулятором по вопросам информационной безопасности в РФ — Федеральной службой по техническому и экспортному контролю (ФСТЭК России). Согласно терминологии ФСТЭК, фактически любая система АСУ ТП, управляющая критически важным объектом или опасным в экологическом плане производством (топливно-энергетического комплекса, транспортной отрасли, атомной промышленности и т.д.), относится к ключевым системам информационной инфраструктуры, или сокращенно КСИИ.

Комплект ФСТЭК по КСИИ включает в себя следующий перечень документов:

- Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры;
- Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры;
- Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры;
- Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры.

Документы ФСТЭК регламентируют технические требования не только к средствам защиты информации, но и к организации процессов управления информационной безопасностью систем АСУ ТП. Например, разработка плана действия в чрезвычайных ситуациях и регламента управления инцидентами также являются неотъемлемой частью обеспечения информационной безопасности систем АСУ ТП. В целом комплект документов по КСИИ представляет собой хорошо структурированный перечень требований и рекомендаций, построенных на основе анализа угроз и степени критичности защищаемой АСУ ТП, отнесенной к КСИИ. Документами предусмотрена классификация систем по назначению и уровням важности.

Требования к защите КСИИ предъявляются на основе отнесения ее к определенному уровню важности и типу. Классификация по КСИИ должна производиться на основании требований документа «Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий», утвержденного секретарем Совета безопасности Российской Федерации.

Вопросы защиты автоматизированных систем управления технологическими процессами важных инфраструктурных объектов актуальны не только в нашей стране. Подтверждением тому является большое количество новых стандартов и лучших практик по информационной безопасности АСУ ТП, выпущенных международными институтами по стандартизации, отраслевыми или государственными организациями.

Причинами подобной активности является высокая степень риска террористической угрозы в современном мире и уязвимость систем АСУ ТП перед современными кибератаками. А успешные атаки на подобные системы на критических объектах могут приводить не только к локальным сбоям в сети предприятия, но и к тяжелым последствиям для региона или государства в целом.

В качестве примера уязвимости систем АСУ ТП можно привести широко обсуждаемый инцидент с атакой иранских ядерных объектов вирусом Stuxnet. Сетевой червь Stuxnet распространялся, используя уязвимости операционных систем Microsoft. При этом целью данного вредоносного кода были системы управления технологическими процессами производства компании Siemens.

Текущая ситуация в России с обеспечением информационной безопасности в технологических сетях АСУ ТП тоже не внушает оптимизма. Уязвимостей в технологических сетях наших предприятий и организаций более чем достаточно. На некоторых объектах

технологические сети являются частью единой офисной сети с подключением к сетям общего пользования. При этом оборудование систем АСУ ТП не имеет практически никаких средств защиты и обновления операционных систем проводятся крайне редко (либо вообще не проводятся). Такое положение делает комплексы АСУ ТП легкой мишенью для атак.

Однако для современных предприятий сложно представить совершенно изолированные сети АСУ ТП. Одной из сегодняшних реалий успешного ведения бизнеса для крупного предприятия является четкая и оперативная вертикаль управления. В том числе, и контроль технологических процессов на региональных предприятиях руководством из центрального офиса. Для реализации безопасного взаимодействия сетей АСУ ТП с корпоративной сетью в центральном офисе предприятия существует специализированное решение одностороннего межсетевого взаимодействия. Решение позволяет передавать данные из технологической сети АСУ ТП в корпоративную сеть, в том числе и оперативную информацию мониторинга по протоколам OPC **(рис.1).**

Данные могут передаваться только в одном направлении: из сети с большей степенью критичности в сеть с меньшей степенью критичности. Это позволяет надежно закрыть канал проникновения вредоносного кода в системы АСУ ТП из внешних сетей **(рис.2).**

Обратное направление информационных потоков невозможно, поскольку физически отсутствует оптический канал приема сигнала на устройстве односторонней передачи. Таким образом, техническое решение одностороннего взаимодействия позволяет обеспечить централизованный оперативный контроль всех производственных процессов территориально-распределенного предприятия при отсутствии угроз проникновения вредоносного кода в системы АСУ ТП через корпоративную сеть и Интернет.

Проблемы в области информационной безопасности технологических сетей АСУ ТП вызваны как объективными, так и субъективными причинами. К объективным можно отнести проблемы, связанные с возможным влиянием средств защиты информации на задержки и время реакции систем АСУ ТП. Многообразие систем АСУ ТП, использование уникальных отечественных разработок, созданных ранее с использованием технологий файлового обмена, действительно иногда не позволяет использовать средства защиты на серверном оборудовании АСУ ТП. Несмотря на подобные факты, большинство систем АСУ ТП не конфликтует со средствами защиты при правильной их установке и конфигурации.

К сожалению, отечественные разработчики систем АСУ ТП не проводят тестирований на совместимость со средствами защиты. Поэтому тестирование совместимости систем ложится на плечи системного интегратора, который внедряет систему обеспечения информационной безопасности. Чтобы обеспечить уверенность в успешном внедрении средств защиты, проводится предварительная отработка применяемых технических решений на полигоне и организация предварительной приемки с приглашением представителей заказчика.

Главным требованием внедрения средств информационной безопасности КСИИ является обеспечение доступности систем АСУ ТП, т.к. чаще всего технологическая информация не является конфиденциальной. Поэтому сохранение уровня отказоустойчивости существующих систем АСУ ТП в технологических сетях и использование средств защиты в режиме горячего резервирования являются одним из приоритетов при создании системы обеспечения информационной безопасности. Сегментирование технологических и информационных сетей с учетом критичности управляемого технологического процесса, уровней важности систем и существующих технологий информационного обмена является также одним из ключевых факторов построения надежной системы защиты.

Рис.1

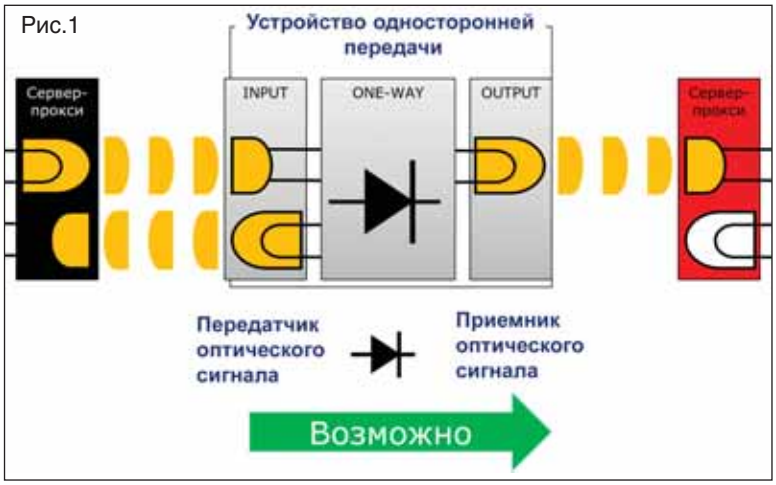

Рис.2