РЕЗОЛЮЦИЯ

Четвертой конференции «Информационная безопасность АСУ ТП критически важных объектов»

17–18 марта в г. Москва состоялась четвертая конференция «ИБ АСУ ТП КВО». В ее работе приняли участие 215 человек. В течение двух дней было заслушано 32 доклада и сообщения, проведен круглый стол по вопросам импортозамещения в сфере АСУ ТП и средств защиты АСУ ТП КВО.

По итогам работы конференции сформулированы следующие предложения и рекомендации.

Общие подходы

- Признать, что риски целенаправленных атак на АСУ ТП КВО возрастают с каждым годом. Необходимые предпосылки для этого (кадры, технические возможности и мотивация) в целом сформировались. Зачастую не требуется высокая квалификация исполнителя, а необходимые инструменты проведения атаки имеются в свободном доступе.
- С учетом наличия тесной связи информационной и промышленной безопасности АСУ ТП признать сложность задачи разработки типовых требований безопасности для всех отраслей промышленности. Рекомендовать учитывать отраслевую специфику при разработке требований к ИБ АСУ ТП. Отметить, что использование типовых решений защиты ограничивает возможности использования АСУ ТП.
- Признать основополагающим принципом защиты АСУ ТП отсутствие (или минимизацию присутствия) воздействия средств защиты информации непосредственно на технологический процесс. Рекомендовать разработчикам и интеграторам средств защиты руководствоваться этим принципом при построении системы защиты АСУ ТП.
- Признать неприемлемой сложившуюся практику замалчивания и крайне медленного исправления ошибок и уязвимостей в программном коде АСУ ТП мировых лидеров.
- Признать, что существующие АСУ ТП часто работают под управлением устаревших операционных систем с большим количеством известных уязвимостей.

Нормативно-правовые аспекты

- Признать отсутствие системного нормативного правового регулирования сферы информационной безопасности АСУ ТП. Необходимо скорейшее принятие Федерального закона «О безопасности критической информационной инфраструктуры РФ» как первоосновы системного подхода в указанном вопросе.
- Поддержать работу ФСТЭК России в части подготовки нормативно-методических документов по информационной безопасности АСУ ТП.
- Рекомендовать предприятиям, операторам критически важных объектов, интенсифицировать работу по реализации приказа № 31 ФСТЭК России.
- Рекомендовать промышленным компаниям, которые не имеют критически важных объектов, также учитывать рекомендации приказа № 31 ФСТЭК России по защите АСУ ТП.
- Рекомендовать компаниям – лицензиатам ФСТЭК России по технической защите информации и компаниям, специализирующимся в области разработки и проектирования АСУ ТП, активнее участвовать в разработке проектов нормативно-методических документов по защите информации и защите систем управления технологическими процессами.

- Рекомендовать операторам КВО при моделировании угроз и оценке рисков учитывать степень доверия к программному и аппаратному обеспечению. Для оценки степени доверия можно использовать такие критерии, как авторство разработки, наличие полной документации в соответствии с ГОСТ ЕСПД и контроль процессов разработки и сертификации уполномоченным государственным органом (ФСТЭК, Минобороны, ФСБ РФ).
- Рекомендовать операторам КВО во взаимодействии со ФСТЭК России, ФСБ России и отраслевыми регуляторами инициировать проработку и реализацию инициатив обмена информацией в области безопасности АСУ ТП, создание центров обмена и анализа информации в области безопасности, центров реагирования на инциденты безопасности и т. п. структур в рамках групп предприятий, вертикально интегрированных объединений, секторов и отраслей промышленности.
- Признать неприемлемой сложившуюся практику, при которой оператор КВО умышленно занижает классность объекта и, как следствие экономит на системе защите АСУ ТП, в том числе на этапе моделирования закладывая в модель угроз наиболее простые типы атак.
- Признать обязательным проведение аудита информационной безопасности во время тестового режима работы АСУ ТП до ее ввода в эксплуатацию
- Рекомендовать службам безопасности на постоянной основе производить мониторинг и инвентаризацию АРМ оператора АСУ ТП. Сложившаяся практика самовольного установления на АРМ оператора непредусмотренного ПО, открытие портов, подключение непредусмотренных регламентом роутеров несут серьезные риски. В качестве эффективной меры борьбы предлагается немедленное изъятие подобных ПК.
- При проведении аудита защищенности АСУ ТП КВО, ввиду отсутствия возможности останова работы технологического оборудования, рекомендовать использовать метод делегации прав на проверку непосредственно персоналу – операторам АСУ ТП.
- Признать необходимость контраварийной подготовки обслуживающего персонала критически важных объектов и дополнить ее базовыми сведениями о защите информации АСУ ТП.
- Рекомендовать операторам КВО интенсифицировать процесс повышения квалификации в области защиты АСУ ТП, в первую очередь среди операторов АСУ ТП.

Поддержка российских разработчиков

- Признать, что на российском рынке не в полной мере представлены все необходимые продукты для защиты АСУ ТП. Рекомендовать разработчикам средств защиты определиться с перспективными технологиями защиты АСУ ТП и включить их в свои планы разработки новых продуктов.
- Признать важность процесса импортозамещения для обеспечения безопасности АСУ ТП КВО. Отметить, что на текущий момент подавляющее большинство внедренных АСУ ТП имеет иностранное происхождение, степень доверия к которому довольно низка в условиях международных санкций.
- Отметить сложность и наличие рисков быстрого перехода на российские аналоги. Учесть тот факт, что иностранные производители имеют большой опыт работы и сопровождения АСУ ТП.
- Рекомендовать отдавать предпочтение российским доверенным продуктам АСУ ТП на новых объектах и при модернизации устаревших при условии качественного сопровождения их со стороны производителей.
- Поддержать инициативу Фонда перспективных исследований по разработке интегрированной инструментальной среды разработки АСУ ТП в качестве одного из возможных вариантов консолидации усилий отечественных разработчиков АСУ ТП. Рекомендовать разработчикам АСУ ТП принять участие в этом проекте.
- Признать, что практика удаленного подключения специалистов производителя промышленного оборудования к АСУ ТП на территории России несет дополнительные риски информационной безопасности. Рекомендовать при невозможности полностью изжить подобную практику ограничить подключение только гарантийным сроком.
- Призвать зарубежных производителей промышленного оборудования начать активное взаимодействие с отечественными разработчиками средств защиты АСУ ТП в части тестирования и гарантирования заказчику безопасности использования продуктов на собственном технологическом оборудовании. Отметить, что за последнее время ряд иностранных производителей приступили к подобному сотрудничеству.
- Рекомендовать производителям промышленного контроллерного оборудования, разработчикам программного обеспечения АСУТП на их основе и средств защиты АСУ ТП усилить совместную работу в целях создания новых или модернизации уже имеющихся инструментов защиты технологических процессов. ■