КИБЕРБЕЗОПАСНОСТЬ СИСТЕМ УПРАВЛЕНИЯ АСУ ТП

СТРАТЕГИЧЕСКИХ ПРЕДПРИЯТИЙ В УСЛОВИЯХ ГЛОБАЛЬНОГО ПРОТИВОСТОЯНИЯ

Главный специалист АО «ИПН» Усачёв В.Ю. info@truboprovod.ru

Обычно безопасность АСУТП (Автоматизированных Систем Управления Технологическими Процессами) исторически рассматривается в контексте надежности/ отказоустойчивости систем и, как правило, сертифицируются по FSS (Functional Safety Standards), а так же по SIL (Safety Integrity Level) для систем ПАЗ (ПротивоАварийная Защита). Но сегодня неотъемной частью общей надежности систем АСУТП становится кибербезопасность. В англоязычных источниках используется термин «cybersecurity», прямой перевод которого (кибербезопасность) все чаще встречается применительно к защите АСУ ТП. Обеспечение безопасности систем АСУТП складывается из 2-х факторов: информационной безопасности (ИБ) и функциональной безопасности (ФБ). Безусловно ИБ очень важна и обычно её считают приоритетной. Однако, есть еще и другая сторона безопасности, связанная с рисками для здоровья и жизни людей, а также окружающей среды. Поскольку информационные технологии сами по себе опасности не представляют, то обычно говорят о функциональной составляющей, то есть о безопасности, связанной с правильным функционированием системы промышленной автоматики. Под функциональной безопасностью (functional safety) подразумевается корректное функционирование, как системы управления, так и управляемого ею оборудования. Таким образом, для обеспечения ФБ необходимо сначала определить функции безопасности, необходимые для снижения риска управляемого оборудования, а также для достижения и сохранения этим оборудованием безопасного состояния (например, функции ПАЗ). Далее, система управления должна обладать свойством так называемой полноты безопасности (safety integrity), под которым МЭК 61508 подразумевает вероятность того, что система будет корректно выполнять функции безопасности при всех заданных условиях в течение заданного интервала времени.

При обеспечении полноты безопасности (safety integrity) учитываются два типа отказов: случайные (random failures) и систематические (systematic failures). Случайные отказы вызваны выходом из строя аппаратных компонентов и парируются такими методами, как резервирование, самодиагностика, физическое и электрическое разделение компонентов, повышение устойчивости к внешним воздействиям и т.п.

Систематические отказы вызваны ошибками проектирования, а также ошибками программного обеспечения. Устранение систематических отказов возможно путем совершенствования процессов проектирования и разработки, тестирования, управления конфигурацией, проектного менеджмента и т.п. Кроме того, поскольку классическое резервирование не позволяет избежать систематических отказов, применяется так называемое диверсное (diversity) резервирование, когда резервные каналы разработаны с применением различного программного и аппаратного обеспечения. Дорого, неудобно, но иногда помогает.

Для управляющих систем, к которым относятся такие архитектуры, как АСУ ТП, встроенные системы, основополагающим свойством является функциональная безопасность (ФБ). Под функциональной безопасностью подразумевается корректное функционирование, как системы управления, так и управляемого ею оборудования.

Информационная безопасность (ИБ) в таких системах носит дополнительный характер и должна предотвращать доступ злоумышленников к контролю над системой управления и управляемым оборудованием.

ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ И ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

- Структурированный процесс разработки системы и программного обеспечения;
- Реализация процесса верификации и валидации, заключающаяся в поэтапном выполнении обзоров, анализа и тестирования, анализ уязвимостей АСУТП;
- Сопровождение продукта после внедрения с учетом обратной связи по результатам эксплуатации;
- Использование лучших практик и стандартов кодирования;
- Использование сертифицированных компиляторов и библиотек;
- Использование типовых языков программирования (стандарт МЭК 61131-3 и т.д.);
- Контроль качества при производстве аппаратных средств;
- Сегментирование сети;
- Исключение беспроводных технологий в промышленных сетях (допускается применение только в нижнем уровене АСУТП: беспроводной датчик – шлюз ввода/ вывода);
- Зонирование размещения оборудования АСУТП;
- Исключение KBM-удлинения посредством корпора-

тивной или общедоступной сети (KVM-over-IP);
- Обучение персонала и развитие культуры безопасности;
- Проведение аудитов на предмет оценки рисков и выявления уязвимостей.

Функциональная безопасность АСУТП это отдельная очень большая и специфичная тема. В данной статье рассмотрим подробнее вопросы именно информационной безопасности АСУТП и систем автоматизации в индустрии, энергетике, транспорте, добыче ресурсов и т.д. в целом.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АСУ ТП

Автоматизированные системы управления технологическим процессом (АСУ ТП) обладают массой отличий от «традиционных» корпоративных информационных систем: начиная от назначения, специфических протоколов передачи данных и используемого оборудования, и заканчивая средой в которой они функционируют. В корпоративных сетях и системах, как правило, основной защищаемый ресурс – информация, которая обрабатывается, передается и хранится в автоматизированных системах, а основные цели – обеспечение ее защиты и конфиденциальности. В АСУ ТП же защищаемым ресурсом, в первую очередь является сам технологический процесс, и основная цель – обеспечить его непрерывность (доступность всех узлов) и целостность (в т.ч. и передаваемой между узлами АСУ ТП информации). Проблема в данном случае не столько в утечке конфиденциальной информации или краже денег со счетов предприятия. В данном случае поле потенциальных рисков и угроз для АСУ ТП, по сравнению с корпоративными системами, расширяется рисками потенциального ущерба жизни и здоровью персонала и населения, ущербу окружающей среде и инфраструктуре, большим материальным потерям в связи с простоями, выпуском бракованной продукции или сокращением выпуска, а так же авариями и техногенными катастрофами. Простой пример экономического ущерба: вследствие некорректной работы АСУ газотурбиной установки (ГТУ) сработали технологические защиты. Из-за остановки ГТУ встал весь энергоблок ГТЭС Повторный запуск мощного энергоблока это сложный и небыстрый процесс. Причем перед пуском энергоблока по регламенту необходимо «прощелкать» все защиты и причем не только на ГТУ, а на всем энергоблоке (котле-утилизаторе, паровой турбине, вспомогательном и высоковольтном оборудовании). Это может занять по времени целые сутки, иногда и больше. За это время остынут паропроводы и их необходимо постепенно разогревать, расходуя пар. В результате незапланированный запуск и вывод на номинальный режим одного мощного энергоблока ТЭЦ или ГРЭС обходится в миллионы рублей. И кроме прямого экономического ущерба есть еще и косвенный – недополученная прибыль из-за недовыдачи электроэнергии в сеть.

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ИБ) АСУТП

- программная самодиагностика;
- защита от вредоносных программ, обнаружение (предотвращение) вторжений;
- сегментирование сети;
- защита периметра сетевыми экранами;
- самодиагностика передачи данных, как по коммуникационным каналам, так и при обработке, распределенной между компонентами программного и аппаратного обеспечение;
- шифрование пакетов передачи данных;
- резервирование данных;
- контроль и управление доступом (физический и программный).

подсистемы обеспечения информационной безопасности АСУ ТП:
- подсистема сетевой безопасности. Иногда ее делят на две системы – межсетевого экранирования и обнаружения вторжений. В таких случаях подразумевается, что в АСУ ТП будет внедрено дополнительное оборудование – межсетевые экраны и система обнаружения вторжений;
- подсистема двухфакторной (многофакторной) аутентификации;
- подсистема обеспечения целостности;
- подсистема быстрого восстановления конфигураций и данных;
- подсистема предотвращения утечек конфиденциальной информации;
- подсистема управления неструктурированными данными;
- подсистема анализа защищенности;
- подсистема криптографической защиты каналов связи (не используется в быстродействующих системах).

Первые три ИБ-подсистемы являются ключевыми в АСУ ТП, поскольку позволяют наиболее эффективно сохранять доступность автоматизированной системы управления. Нужно отметить, что российский рынок решений для информационной защиты автоматизированных систем управления и индустриальных сетей находится в зачаточном состоянии. Каждый конкретный проект подразумевает сугубо индивидуальное решение. Кроме того, обеспечить безопасность АСУ ТП исключительно с помощью серийных технических средств крайне сложно. Дело в том, что специфика АСУ ТП не позволяет использовать стандартные ИБ-решения для других IT-систем. Если для стандартной IT-системы приостановка какого-то процесса в случае подозрения на вредоносную активность является нормальной мерой, то в промышленных систем это может стать причиной техногенной катастрофы.

НОРМАТИВНЫЕ ДОКУМЕНТЫ В ОБЛАСТИ ИБ И ФБ СИСТЕМ АСУТП

- Приказ ФСТЭК России №31 от 14.03.2014 "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".
- Закон №256-ФЗ «О безопасности объектов ТЭК».
- ГОСТ Р МЭК61508-2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью».
- ISA/IEC 62443 серия стандартов Security for industrial automation and control systems.

Так же к нормативным документам, регламентирующим Информационную безопасность не только АСУТП, но и более широкого применения, можно отнести следующие:
- Информационное сообщение ФСТЭК России от 28 апреля 2016 г. N 240/24/1986 «Требования к межсетевым экранам».
- ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования.
- ГОСТ Р ИСО/МЭК 27034 Информационная технология (ИТ). Методы и средства.

ПРОБЛЕМЫ В ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ ТП

Важно отметить, что приказ №31 ФСТЭК хоть и является важным документом в обеспечении ИБ АСУ ТП критически важных объектов, но, по сути, не носит обязательного характера к применению для организаций, в чьем ведении такие объекты находятся. Данный документ применяется при принятии владельцем АСУ (Заказчиком) решения о необходимости и «полноты» защиты информации в проектируемой системе.

Большинство представленных на российском рынке ИБ-продуктов адаптированы для защиты зарубежных АСУ ТП (базовых ПО), но не сертифицированы по требованиям нашего законодательства, поскольку зарубежные поставщики не всегда готовы предоставлять исходные программные коды своих продуктов, что необходимо для сертификации. Отечественных же ИБ-решений требуемого уровня пока нет (приятное исключение, пожалуй, только некий набор программных продуктов Kaspersky Industrial CyberSecurity от компании «Лаборатория Касперского»).

Типовые проблемы в организации информационной безопасности АСУ ТП на действующих промышленных объектах:

• Отсутствие какой-либо организации в решении вопросов безопасности АСУ ТП. Зачастую само понятие информационной безопасности АСУ ТП на объекте не используется и ответственность за ее обеспечение ни на кого не возложена.

• Нет организационно-распорядительной документации по обеспечению ИБ в АСУ ТП, а корпоративные процессы и процедуры безопасности эту систему не затрагивают.

• Отсутствие требований по ИБ или их несоблюдение со стороны персонала, эксплуатирующего промышленные системы.

• Низкий уровень компетенции в вопросах ИБ у специалистов по автоматизации, внедрению, эксплуатации, обслуживанию.

• Слабая осведомленность в вопросах автоматизации у специалистов по ИБ, как правило, это просто IT-специалисты.

• Частичное или полное отсутствие документации на используемую АСУ ТП. Система в эксплуатации не первый десяток лет, документы потерялись, было много доработок, люди, стоявшие у истоков, уволились, и теперь никто толком не знает, как она работает.

• Непонимание целей проведения работ, расхождение между утвержденным заданием и ожиданиями заказчика, а также отсутствие понимания между функциональными подразделениями. При этом попытки наладить взаимодействие различных подразделений предприятия не предпринимаются.

• Неконтролируемый доступ к технологическим системам и отсутствие контроля за действиями подрядчиков и используемыми каналами удаленной связи с разработчиками АСУ ТП.

• Часто устаревшее морально технологическое и ИТ/сетевое оборудование.

• Отсутствие контроля доступа к компонентам АСУТП и сетевому оборудованию. Упрощенная или отсутствие аутентификации, пароли по умолчанию или хранение паролей в доступном месте.

• Отсутствие антивирусной защиты, каких-либо обновлений и контроля съемных носителей в технологической среде, использование устаревших ОС.

• Бесконтрольный доступ к системе и сетевым компонентам АСУТП подрядчиков для проведения различных регламентных, сервисных и др. работ со своими ноутбуками.

На сегодняшний день существуют ИБ-средства, “заточенные” под особенности АСУ ТП, — специализированные межсетевые экраны, средства защиты межсетевого взаимодействия типа “диодов данных” (Data diode), обеспечивающие на физическом уровне однонаправленную передачу данных между технологическим сегментом и остальной корпоративной сетью. Базами уязвимостей компонентов АСУ ТП, а также необходимой поддержкой промышленных протоколов сегодня обзавелись системы обнаружения и предотвращения вторжений и анализа защищенности.

Важно отметить, что компоненты обеспечения безопасности АСУТП (и на аппаратном уровне и на программном уровне) не дёшевы и заметно удорожают общую стоимость проектируемой системы. Заказчик, в целях минимизации бюджета строительства/реконструкции объекта стремится приобрести АСУТП за минимальные деньги (из всех участников тендера), но при этом требует обеспечение ИБ и ФБ приобретаемой системы. Можно, конечно создать ну очень «навороченную» систему безопасности проектируемой АСУТП: это и межсетевые экраны (файрволы) на каждом шагу, и создание виртуальной DMZ-зоны на границе 2-го и 3-го уровня модели АСУ предприятия (MES-системы) с промежуточными (прокси)серверами «доверия». Как говорится: «Нет предела совершенству». Но насколько все это нужно заказчику и сколько он готов переплатить за безопасную АСУТП?

Наиболее надежный простой и дешевый способ обеспечить ИБ проектируемой АСУТП в части сетевых коммуникаций с другими сетями и системами предприятия это внедрение средств однонаправленной передачи данных. Их ключевая особенность в том, что пакеты данных физически могут передаваться только в одну сторону (из проектируемой АСУТП), что является абсолютной защитой от внешнего сетевого воздействия. Другой вопрос: Устроит ли данное техническое решение Заказчика.

Обеспечение комплексной системы безопасности АСУТП лежит на:
- заказчике, в период эксплуатации уже внедренной АСУТП (управление доступом, обучение персонала, обновление ПО, резервное копирование данных и т.д);
- и на проектной компании разработчике ТЗ на АСУТП

совокупно с системным интегратором (разработчиком и поставщиком ПТК) на стадии проектирования системы: аппаратное и программное резервирование, сетевое резервирование, сегментация сети, SIL, соответствующе сертифицированное ПО и оборудование и т.д.
Итак, мы обсудили обеспечение комплексной информационной безопасности АСУТП от угроз приходящих, так сказать, «извне» -вторжения, кибератаки, халатное отношение проектировщиков, эксплуатирующего персонала и их подрядчиков. Этой теме в последнее время посвящено много публикаций, проводятся конференции, в т.ч. международные, выпускаются правительством постановления и др. нормативные документы, есть уже и определенные наработки, например у Лаборатории Касперского и у НПФ «Круг», то есть дело потихоньку двигается в сторону улучшения ситуации. Но хотелось бы заострить внимание еще на одном аспекте информационной безопасности, на которое или не обращают внимание, или же считают эту угрозу «мифической», или же не предполагают такого коварства от наших международных «партнеров», но которую нигде особо в публикациях и на конференциях не обсуждают, не отражена она (угроза) и в нормативной документации. По опыту автора: обсуждается эта тема иногда только между коллегами АСУшниками на бытовом уровне, да пару раз встречалась на специализированых форумах в интернете. Это потенциальная угроза, связанная с поставкой импортного сложного технологического оборудования комплектного с собственной системой управления (САУ, ЛСУ, МСУ и тому подобные) и собственным ПО. Например,комплектная поставка мощного дожимного газового компрессора или установки гликолевой осушки газа или же газопоршневой или газотурбинной генераторной установки (ГТУ). В зависимости от мощности и сложности установки, иногда они поставляются с системой управления, расположенной в нескольких двухметровых шкафах, напичканных электроникой, с «залитой» в их контроллеры и серверы сложной прикладной программой.

«БАГИ» - СПЯЩИЕ АГЕНТЫ

Прежде чем начать обсуждение этой темы и чтобы понять всю серьезность потенциальной угрозы, хочу привести одну цитату официального государственного деятеля - первого заместителя министра обороны США Уильяма Линна (William J. Lynn). Цитата: «Первый из этих принципов заключается в том, что мы должны признать киберпространство тем, чем оно уже стало – новой зоной военных действий. Точно так же, как сушу, море, воздушное и космическое пространство, мы должны рассматривать киберпространство как сферу наших действий, которую мы будем защищать и на которую распространим свою военную доктрину. Вот что побудило нас создать объединенное Киберкомандование в составе Стратегического командования. Второй принцип, о котором я уже упоминал — оборона должна быть активной.» и т.д. В США создан, по сути, отдельный род войск. Президент США Дональд Трамп своим указом присвоил Киберкомандованию (Cyber Command) статус единого боевого командования. Американская армия ранее насчитывала девять единых боевых командований. Из них шесть были региональными: Европейское, Центральное, Африканское, Тихоокеанское, Североамериканское и Южное. Ещё три командования было выделено по исполняемым функциям: Стратегическое командование (объединяет силы ядерного сдерживания, ПРО и управление военными космическими средствами), Командование сил специальных операций и Транспортное командование. Киберкомандование вооружённых сил США ранее входило в состав Стратегического командования и носило статус sub-unified combatant command. Теперь же статус «кибервойск» изменён на unified combatant command, что делает Киберкомандование равноправным с бывшей курирующей структурой.
Итак, у нашего потенциального противника имеются специализированные военные подразделения для ведения боевых действий в «электронно-программной сфере». Как известно, военные в мирное время преимущественно занимаются тем, что готовятся к будущей войне. Чем же занимаются военнослужащие этих подразделений? Вряд ли они отрабатывают на полигонах тактику ведения пехотного боя и проводят время на стрельбищах. В современных войнах и локальных конфликтах противоборствующие силы стремятся наряду с нанесением максимального урона военным силам противника, так же стараются максимально ослабить его промышленный потенциал. И не только предприятия ВПК или двойного назначения, но и энергетику, транспортную инфраструктуру, нефте-газопроводы, стратегические предприятия машино- и станкостроения, металлургию и т.д.
Автор, много лет проработал в компании, которая занималась инжинирингом и поставкой оборудования для газопереработки, энергетики, нефтехимии из США, Германии, Италии. Видел следующую картину: все поставляемое технологическое оборудование нашими российскими соответствующими органами досконально проверялось, сертифицировалось; назначались экспертизы, проверялись документация, сертификаты, клеймо ASME и т.д. Но вот системы управления с прикладным ПО, комплектно поставляемые с этим технологическим оборудованием, особо не проверялось и не анализировалось. Только формально: предоставить международные сертификаты и мануалы на КИП и контроллерное оборудование, ну и по взрывозащите полевого КИП. Система управления была, как бы, «черный ящик» в который лучше не соваться. Производитель гарантировал, что под её управлением вся технология будет работать в соответствии с требованиями заказчика. К тому же на период пуско-наладки от производителя/поставщика установки приезжал специалист или насколько специалистов, которые в том числе конфигурировали, настраивали и решали все вопросы связанные с АСУ поставленной их компанией технологической установки. А что там «зашито» в прикладном ПО? Какие микросхемы и микроконтроллеры стоят в электронных модулях и блоках? Никто не интересовался. Отладили, запустили, все работает- вот и хорошо. Можно спать спокойно.
Но так ли все спокойно и безопасно? Где гарантия, что в поставляемой из стран членов НАТО и других стран, не членов НАТО, но союзников США (Япония, Тайвань, Швеция и т.д.), в оборудовании и ПО не дремлет и не ждет своего часа вредоносный «жучек»? Допустим в прикладном ПО, в одном из многочисленных алгоблоков (может маскироваться под дата-блоки, фанкшен-блоки,

отдельные скрипты) запрятан некий вредоносный код, который активизируется по определенному сигналу. А в аппаратной части (HW – HardWare, т.е. контроллер, модули ввода/вывода, интерфейсные и т.д.), внутри какого-нибудь модуля или электронного блока среди множества электронных элементов находится неприметная микросхемка, которая способна принять радиосигнал (даже можно допустить что что это будет определенный код по сотовой сети 3G/4G/5G) и которая приняв этот сигнал из радиоэфира, выдает внутрисистемный сигнал на активизацию вредоносного кода в прикладном ПО, которое также было разработано и поставлено нам (причем куплено нами за весьма немалые деньги) в стране – потенциальном военном противнике России. А почему нельзя исключать такой вариант? Технически это сделать абсолютно реально, современные технологии это позволяют. А обнаружить это крайне сложно (об этом ниже), да этим и никто не занимается. Если проводить аналогию с терминологией спецслужб, то это получается аналог спящей террористической (диверсионной) ячейки. Но с таким «спящим агентом» вредоносным жучком (будем называть его «баг» от англ. Bug - жучек) для нашего потенциального противника задача намного упрощается:

- не надо изготавливать и доставлять взрывчатку,
- не надо проникать на охраняемый объект (завод, объект энергетики, масторождение, нефте- или газоперекачивающую станцию и т.д.), заказчик сам «доставит и внедрит» бага себе в АСУТП,
- не надо платить деньги спящей ячейке или спящему агенту,
- не надо никаких сложных и дорогих конспиративных действий и мероприятий,
- в случае провала спящий агент не «расколется» и не сдаст агентурную сеть.

Начиная примерно с начала нулевых годов наша страна активно закупала в западных странах высокотехнологическое оборудование для своей промышленности. На это были объективные причины: это и общее технологическое отставание, и то что наша собственная промышленность была в упадке после 90-х, и активная маркетинговая политика западных компаний, да и коррупционная составляющая, надо признать, имела место. В результате мы имеем то, что практически на всех современных или модернизированных предприятиях в нефте-газовом секторе и в энергетическом секторе (возможно и в других производственных секторах, просто автор работал и знает сложившуюся ситуацию именно в этих сферах), имеется как минимум один технологический блок или установка, поставки западной компании со своей ЛСУ (Локальная Система Управления, может еще применяться термин САУ – система автоматического управления), имеющие критическое значение для всей технологической цепочки предприятия в целом. Например, возьмем мощную ГТЭС (ТЭЦ, ГРЭС). На её территории среди огромных цехов (котельных, турбинных), высоких дымовых труб и огромных парящих градирен находится относительно небольшое здание ДКС (дожимная компрессорная станция). ДКС нужна, чтобы подать газ в энергетическую турбину, преодолев противодавление в её камере сгорания. Остановятся газовые компрессоры в ДКС и «потухнет» вся станция ГТЭС. Сотни мегаватт, а то и более тысячи мегаватт перестанут поступать в энергосеть. А ведь в нашей стране сейчас на подавляющем большинстве ГТЭС газовые компрессоры производства США, западноевропейских стран, Японии, Ю.Кореи и, как правило, со своими собственными САУ/ЛСУ. Еще пример: Газоперерабатывающий завод (ГПЗ). В начале технологической цепочки находится установка гликолиевой осушки газа (УОГ) производства США. Установка сложная высокотехнологичная и,соответственно,со своей САУ. Остановится УОГ – остановится весь ГПЗ. Аналогичный пример можно привести для НПЗ и т.д. Оппоненты могут возразить: критически важные агрегаты и установки на производстве всегда проектируются так чтобы был резервный агрегат или установка параллельно основному и между ними реализован АВР. Например: остановился основной насос перекачки нефти – автоматически запустился резервный. Все, можно спать спокойно. Но дело в том, что всегда, подчеркну – всегда, при проектировании и поставке резервный и основной агрегаты заказываются у одной и той же компании, по одному и тому же опросному листу, в одном ордере и поставляются в одной партии. И если уж производитель заложил «баг» в основной агрегат, то он заложит «баг» и в резервный. И в час «Ч» одновременно активируются оба «бага» – и в основном, и в резервном агрегатах.

Но это еще не все. Вредоносный код может не только остановить и заблокировать работу или даже вызвать аварию отдельной технологической установки/агрегата, но и пойти дальше. Часто локальные САУ интегрируются в АСУТП посредством интерфейсных связей для обмена данными по стандартным промышленным протоколам. Если связи осуществляются физическими сигналами, т.е. дискретными или аналоговыми, то тогда проблем нет, но по интерфейсным связям активированный цифровой вредоносный код попадает в вышестоящую АСУ, например АСУТП цеха, или АСУТП энергоблока. А если пораженная АСУТП принадлежит установке, находящейся в начале технологической цепочки всего предприятия, например установка первичной переработки нефти ЭЛОУ на НПЗ, то тогда может встать и весь нефтеперерабатывающий завод, по крайней мере большая его часть.

Итак, мы имеем безрадостную картину: в начале войны (или в предвоенный период) с нашими западными «партнерами», в нашей стране могут разом остановиться большинство электростанций, большинство НПЗ и ГПЗ, большинство газоперекачивающих и нефтеперекачивающих станций трубопроводной системы. Возможно остановятся и другие стратегические объекты, автор просто не знаком с ситуацией в других отраслях. Проблема, как мы видим стратегическая и значит решать её надо на государственном уровне.

СЕРТИФИКАЦИЯ ИМПОРТНОГО SW И HW

Как упоминалось выше, автор ни разу не сталкивался с тем, чтобы кто-то проверял и сертифицировал у нас иностранное прикладное программное обеспечение (SW- SoftWare) и аппаратную часть (HW – HardWare). Правда для этого есть объективные причины.

- Во-первых, что касается SW: производитель разработчик прикладного ПО должен предоставить доступ ко всем алгоблокам и кодам своей программы. Но проблема в том, что часто программа, управляющая сложной

установкой с уникальным технологическим процессом, является ноу-хау и интеллектуальной собственностью разработчика и производителя. Просто так по первому требованию никто раскрывать свою программу не будет. К тому же это может повлечь проблемы в юридическом плане и бюрократические проволочки. Часто в алгоблоках прикладного ПО к какой-то конкретной технологической установке или агрегата «зашит интеллектуальный труд» десятков и сотен человек, месяцы экспериментальных наработок и годы практической эксплуатации этой установки на различных режимах. Часто там алгоритм строится на эмпирических данных, которые невозможно рассчитать математически или иным научным путем, а только на данных полученных компанией производителем за годы выпуска и последующей эксплуатации этого технологического оборудования.

- Во-вторых, что касается HW: разработчик-производитель контроллерного оборудования, использованного в шкафах САУ установки должен предоставить принципиальные электрические схемы и монтажные схемы печатных плат с подробной спецификацией всех электронных компонентов. А это все тоже является ноу-хау и интеллектуальной собственностью разработчика и производителя электронного оборудования. Возникают проблемы, такие же как в предыдущем пункте. Но мало иметь просто всю информацию по поставляемому HW, необходимо будет реально руками разобрать все поставляемые электронные блоки и модули и проверить на предмет соответствия всех электронных элементов предоставленным схемам и спецификациям. Нет ли «лишней» микросхемки в дальнем углу печатной платы? А кто же из производителей потом даст гарантию на свою продукцию, когда кто-то, пусть даже высококлассный специалист-электронщик, разобрал и потом собрал их электронный девайс?

- В-третьих, экономическая составляющая. Даже если производители предоставят всю требуемую информацию, то кто будет заниматься анализом всей этой информации и кто будет финансировать? Для этого потребуются высококлассные специалисты: программисты, электронщики, тестировщики программных продуктов. Это высокооплачиваемые специалисты, работающие на дорогом оборудовании с лицензионным ПО, требующем регулярной оплаты. И быстро такую сложную высокоинтеллектуальную работу не проведешь. В зависимости от сложности ПО, работа может растянуться на месяцы. Все это выливается в приличную сумму. Будет за это переплачивать российский заказчик технологической установки/агрегата чтобы потом спать спокойно? Автор сомневается в этом, особенно глядя на стратегию наших «эффективных менеджеров», ничего не смыслящих в технике, но умеющих хорошо считать деньги на калькуляторе и управляющие при этом крупными заводами и предприятиями. Будет ли за это платить иностранный поставщик ? После того как он будет вынужден раскрыть все свои инженерные и программные разработки и опытно-исследовательские наработки (ноу-хау), которые потом могут попасть к его конкурентам, еще потом и платить за это «удовольствие»? Тоже вряд ли.

Как выход в этом случае? Автор не берется делать какие-либо однозначные выводы, но ясно одно: проблема очень серьезная, касающаяся стратегической экономической безопасности нашей страны и решать её уже пора. Решать пора на государственном уровне. С созданием единого государственного центра сертификации иностранных индустриальных автоматизированных систем управления и, возможно, с частичным государственным финансированием. Решать надо, пожалуй, на законодательном уровне, жестко обязывающем всех участников процесса обязательно проходить сертификацию, предоставлять всю необходимую информацию, государство в свою очередь должно гарантировать разработчику сохранность его ноу-хау и интеллектуальной собственности. Подобную структуру, например, можно создать на базе хорошо зарекомендовавшей себя Лаборатории Касперского.

С 1 января 2018 года вступил в силу закон «О безопасности критической информационной инфраструктуры», обязывающий собственников/управляющие компании принимать организационные и технические меры по обеспечению информационной безопасности на должном уровне. Этот документ описывает основные принципы, по которым государство будет выстраивать систему контроля и мониторинга информационной безопасности на объектах критически важной инфраструктуры. Контроль за исполнением закона поручены ФСБ и ФСТЭК России.

Прошло уже почти 5 лет после принятия этого закона. И как обстоят дела? По отчетам и докладам все хорошо. Но на действующих предприятиях, подразделениям автоматизации / АСУТП заниматься этим некогда – у них производство, план. Государственных проверяющих, контроллеров в сфере ИБ АСУТП там как правило никто и не видел, по крайней мере автору это не известно. Руководители этих подразделений считают, что уж их-то эти напасти («баги», вредоносное ПО и т.д.) не коснутся – ведь раньше не случалось, значит и не будет. Но все «до поры, до времени».

В идеале, конечно, надо самим в России разрабатывать и производить все требуемое технологическое оборудование со своим SW и HW, но пока, к сожалению, сохраняется технологическое отставание России от ведущих западных стран в сфере микроэлектроники, а наша промышленность не может нормально развиваться без современных технологий, решать эту непростую проблему необходимо государству на законодательном уровне и реально контролировать ситуацию и исполнение действующих нормативно-правовых документов в сфере ИБ, в том числе в области АСУТП на предприятиях промышленности, энергетики, транспорта, ТЭК и т.д.

Необходимо отметить,что в России уже не первый год успешно работают несколько отечественных компаний,обеспечивающих потребности нефтяных,газовых и других промышленных предприятий оборудованием и прогаммным обеспечением для автоматизированных систем управления технологическими процессами.Например,НПФ «КРУГ» уже успешно реализовало в полном объёме сотни АСУ ТП на предприятиях нефте- и газопереработки,электростанциях и других промышленных предприятиях.С отечественными компаниями вопросы кибербезопасности решаются проще,их можно практически полностью контролировать.