Актуальные вызовы и адекватные подходы к обеспечению информационной безопасности АСУТП

И.А. Бадеха (ЗАО «Ай-Теко»)

Анализируются вопросы нормативно-правового регулирования в области информационной безопасности (ИБ) АСУТП. Рассматривается подход к оценке рисков ИБ АСУТП, связанный с выполнением злоумышленниками целенаправленных атак, основанный на построении деревьев атак. Перечислены ключевые технические механизмы обеспечения ИБ АСУТП.

Ключевые слова: информационная безопасность, нормативно-правовое регулирование, построение деревьев атак, межсетевое взаимодействие.

Введение

Вопросы обеспечения ИБ АСУТП становятся все более актуальными как в связи с ростом интереса злоумышленников к АСУТП, так и в связи с развитием самих АСУТП, включая:

1) рост потребностей интеграции АСУТП в единую корпоративную систему, связанных, например, со сбором исторических данных, мониторингом состояния АСУТП, передачей производственных параметров, с созданием центров управления производством уровня завода;

2) передача обслуживания инфраструктуры АСУТП на инсорс/аутсорс, в том числе с возможностью удаленного подключения через Internet;

3) постепенный переход на использование стандартных протоколов на базе Ethernet на «низком» уровне автоматизации;

4) развитие полевого уровня АСУТП: повышение «интеллекта» полевых устройств, использование радиоканала на полевом уровне.

Ведущие мировые державы активно занимаются изучением возможностей по проведению атак на промышленные, финансовые и иные ключевые объекты с использованием информационных технологий. Так, Министерством внутренней безопасности США с 2006 г. проводятся учения Cyber storm, отчет о которых выкладывается в открытом доступе. В России в 2014 г. созданы «войска информационных операций», в США и Китае подобные кибервойска существуют уже несколько лет и регулярно проводят учения.

При формировании подходов к обеспечению ИБ АСУТП приходится учитывать разнообразие архитектурных, функциональных и прочих особенностей АСУТП. Следует также учитывать, что ИБ АСУТП, как и ИБ в целом, должно начинаться с:

1) структурирования процессов обслуживания АСУТП, в результате которого они должны стать прозрачны и однозначно воспринимаемы, при этом ответственность должна быть четко распределена между участниками этих процессов,

1) выделения (физического, виртуального, организационного) технологической сети и отделения ее от корпоративной ЛВС.

Выбор механизмов по обеспечению ИБ АСУТП существенно зависит от возможных последствий ее нарушения, то есть степени априорного риска объекта. Опыт многих предприятий показывает, что вопросы обеспечения безопасности, в том числе и информационной, осознаются руководством предприятий в той или иной мере, при этом в зависимости от степени опасности автоматизируемого процесса и соответственно априорного риска АСУТП различается и минимальный адекватный уровень степени зрелости оператора АСУТП.

Далее рассмотрим особенности нормативно-правового регулирования в области ИБ АСУТП и основные апробированные подходы к обеспечению ИБ АСУТП с учетом особенностей данных систем.

Нормативно-правовое регулирование в области ИБ АСУТП

Нормативно-правовая база в области ИБ АСУТП на сегодняшний день, очевидно, недостаточна, поскольку отсутствуют действующие законодательные требования, которые заставляли бы операторов АСУТП заниматься их защитой. Ниже перечислены верхнеуровневые документы, затрагивающие вопросы ИБ АСУТП:

1. Стратегия национальной безопасности РФ до 2020 г.

2. «Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ» (утв. Президентом РФ, 03.02.2012 г. № 803).

3. Указ Президента РФ от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ».

Кроме того, выдвигался ряд законопроектов по этой теме:

1. «Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры», 2006 г.;

2. «О безопасности критической информационной инфраструктуры РФ», 2013 г.;

3. «О внесении изменений в законодательные акты РФ в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры РФ», 2013 г.

Вместе с тем существует отраслевое регулирование вопросов безопасности АСУТП, например, для объектов топливно-энергетического комплекса, для объек-

тов, связанных с использованием атомной энергии, для транспортной отрасли. Эти случаи не изменяют общей картины, так как либо не содержат глубоко проработанных требований по обеспечению ИБ (например, для объектов ТЭК), либо относятся к узкому классу объектов и опираются на методы обеспечения ИБ, основной целью которых является максимальное ограничение обработки информации (например, обязательное требование гальванической развязки, предпочтение организационным мерам защиты), что не всегда приемлемо.

Однако нельзя не отметить, что усилиями ФСТЭК России с участием профессионального сообщества создана адекватная методическая база по обеспечению ИБ АСУТП, а именно:

1. Приказ ФСТЭК России № 31 от 14 марта 2014 г. «Об утверждении требований по защите АСУТП...», согласно которому:

a. требования применяются в случае принятия владельцем АСУТП решения об обеспечении защиты информации, обработка которой осуществляется этой системой ...;

b. требования зависят от класса защищенности, который определяется отдельно для каждого из уровней (операторского (диспетчерского) управления, автоматизированного управления, ввода/вывода данных, исполнительных устройств) и сегментов АСУТП.

2. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007).

3. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007 г.).

В документах ФСТЭК России фактически введено понятие критически важной информации АСУТП, к которой относятся следующие виды информации: управляющая, контрольно-измерительная, программно-техническая, иная информация ограниченного доступа.

Кроме того, для обеспечения ИБ АСУТП могут использоваться международные стандарты, среди которых:

1) NIST SP 800-82 «Guide to industrial Control Systems (ICS) Security»;

2) ISA/IEC-62443, Industrial Automation and Control Systems Security (IACS);

3) NERC CIP, Cyber Security.

Таким образом, на текущий момент существует достаточно обширная методическая база по обеспечению ИБ АСУТП, но при этом отсутствуют законодательные требования по применению тех или иных подходов. Складывается ситуация, при которой государство может оказаться не готовым к актуальным геополитическим вызовам, связанным с кибербезопасностью.

При этом законодательство РФ в области промышленной безопасности, где государственный контроль и надзор осуществляет Ростехнадзор, намного более развито. В частности, Федеральный закон от 21.07.1997 г. № 116-ФЗ «О промышленной безопасности опасных производственных объектов» оперирует такими понятиями, как:

Если лобовая кибератака не удалась, то надо переходить к мозговому штурму.
Журнал "Автоматизация в промышленности"

– *«авария»* (разрушение сооружений и (или) технических устройств, применяемых на опасном производственном объекте, неконтролируемые взрыв и (или) выброс опасных веществ);

– *«инцидент»* (отказ или повреждение технических устройств, применяемых на опасном производственном объекте, отклонение от установленного режима ТП). Инциденты и аварии на опасных производствах могут происходить, в том числе и в результате нарушения информационной безопасности.

В связи с вышесказанным представляется достаточно обоснованным дополнение законодательства в области промышленной безопасности положениями об обязательности выполнения тех или иных требований в области информационной безопасности в зависимости от категории опасности объекта.

Подходы к обеспечению и управлению ИБ АСУТП

Международные стандарты как в области обеспечения и управления ИБ (в частности, из серии ISO 27000), так и в области обеспечения и управления ИБ АСУТП (например, NIST SP 800-82) базируются на процессном подходе. Например, реализуются следующие процессы управления ИБ АСУТП: управление рисками ИБ АСУТП, аудит обеспечения ИБ АСУТП, мониторинг требований законодательства, оценка эффективности, подтверждение и планирование обеспечения ИБ АСУТП, планирование непрерывности функционирования АСУТП.

В рамках процесса управления рисками оцениваются риски различного рода, в том числе:

1) связанные с выполнением злоумышленниками целенаправленных атак (возможности зависят от конкретных нарушителей, признанных актуальными);

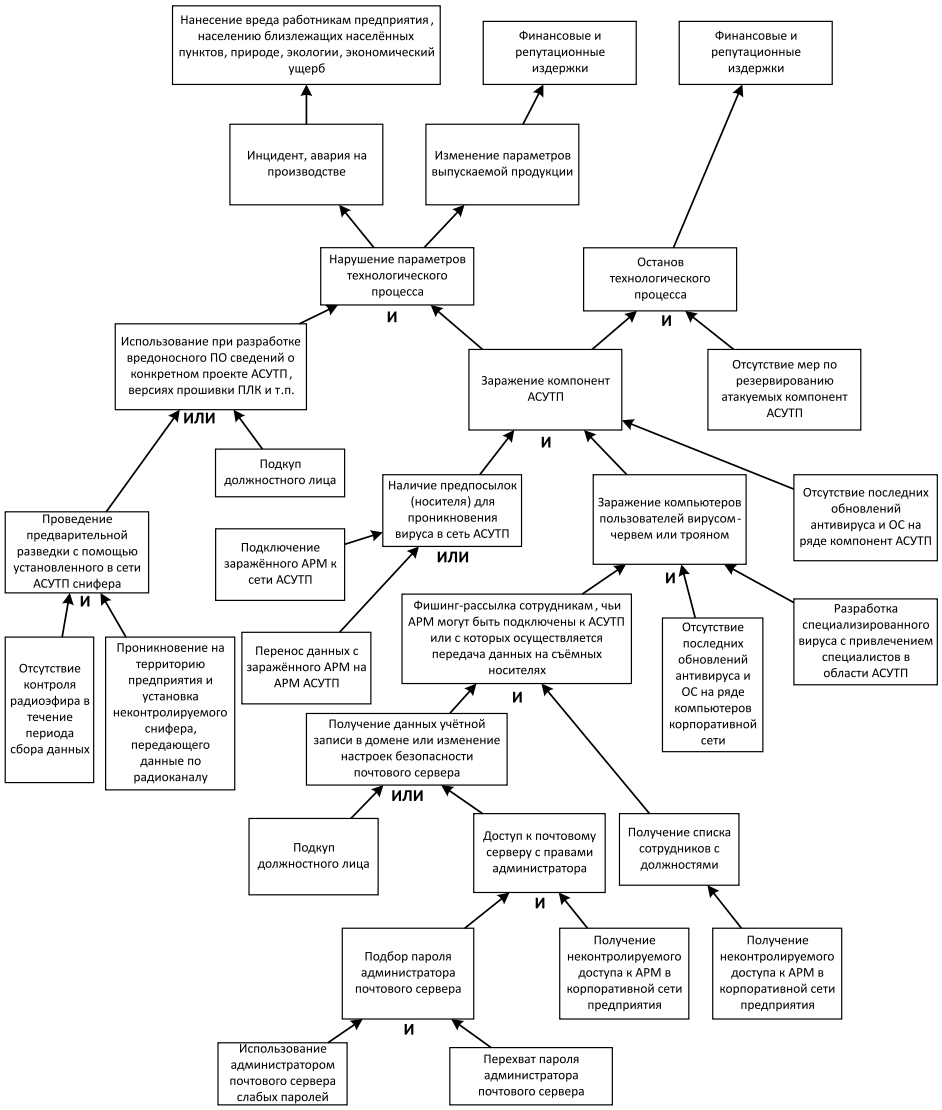
2) связанные с ошибочными действиями персонала и с нарушением персоналом предписаний и установленных правил ИБ;

3) связанные с ошибками при проектировании АСУТП;

4) не связанные с действиями человека.

Следует учитывать, что с точки зрения ИБ для критически важной информации АСУТП, как правило, требуется обеспечить такие параметры, как целостность, доступность, неотказуемость (особенно для управляющей информации). Конфиденциальность при этом обеспечивается, в основном, в целях противодействия разведывательным действиям нарушителя по подготовке к проведению атак на АСУТП.

Для снижения рисков, не связанных с действиями человека, используются стандартные подходы, включающие архитектурные решения по резервированию оборудования и каналов связи, процедуры восстановления данных и компонентов системы и т.п. При этом используются и механизмы, предлагаемые



Пример результатов проработки сценария атаки на АСУТП предприятия

производителями ПЛК и других компонент АСУТП, включая программные технологии резервирования контроллеров. Кроме того, предотвратить последствия от реализации подобных рисков призвана система автоматической защиты.

Риски, связанные с ошибочными действиями персонала, снижаются, в первую очередь, мерами по детальному журналированию действий персонала и установлению персональной ответственности за совершенные действия.

Риски, связанные с ошибками проектирования, могут выявляться путем проведения дополнительных экспертиз, а также путем моделирования последствий выполнения сценариев, приводящих к реализации того или иного риска.

При оценке рисков ИБ АСУТП, связанных с выполнением злоумышленниками целенаправленных атак, апробирован и успешно применяется подход, основанный на построении деревьев атак (например, [1]). При построении дерева атаки каждая его вершина ставится в соответствие некоторому промежуточному этапу атаки, а корень — основному результату атаки. Вершины, соседние с данной вершиной дерева и находящиеся дальше от его корня, сопоставляются этапам, которые предшествуют выполнению этапа, сопоставленного данной вершине. При этом логически предшествующие этапы иногда должны выполняться одновременно (логическое «И»), а иногда достаточно выполнения одного из предшествующих этапов (логические «ИЛИ»). Любая цепь дерева, одним из концов которой является его корень, сопоставляется в этом случае отдельному сценарию реализации атаки. При построении дерева сразу отбрасываются наименее вероятные или почти тождественные сценарии.

На рисунке приведен пример результата проработки сценария атаки, представленного в виде дерева атак, дополненного указанием возможных последствий реализации такого сценария.

Каждой вершине такого дерева сопоставляются определенные (как технические, так и организационные) меры защиты, которые позволяют исключить или затруднить возможности развития соответствующего сценария развития событий.

Применение подхода оценки рисков на базе дерева атак позволяет аргументировано использовать системы сбора и анализа корреляции событий (например, системы класса SIEM) для своевременного выявления начавшейся атаки и планирования действий по предотвращению дальнейшей реализации сценариев, приводящих к наиболее опасным последствиям. На примере приведенного выше фрагмента видно, что корпоративная сеть должна являться первым «рубежом» защиты АСУТП, поэтому при создании системы сбора и анализа корреляции событий для сети АСУТП в качестве источников данных следует рассматривать и источники в корпоративной сети.

Для построения леса реализуемых атак может использоваться тест на проникновение, но при этом он применяется точечно и с выполнением всех возможных предосторожностей, например с созданием объектов, дублирующих выбранные компоненты инфраструктуры на техническом и программном уровне, но не способных повлиять на технологические процессы.

Вектор атаки может быть направлен как «сверху-вниз» (наиболее часто рассматриваемая ситуация, при которой злоумышленник проводит удаленную атаку из внешней сети), так и «снизу-вверх» (в этом случае злоумышленник пользуется возможностью неконтролируемого физического доступа к компонентам нижнего уровня автоматизации (например, уровень ввода/вывода) и уязвимостями протоколов нижнего уровня). В обоих случаях необходимо иметь средства, позволяющие отследить инцидент, являющийся этапом реализации сценария какой-либо из атак.

Среди факторов выбора организационных технических мер защиты – степень риска АСУТП на каждом конкретном технологическом участке, архитектурные особенности АСУТП, наличие технологической потребности в обмене данными и в удаленном доступе, наличие мобильного доступа, наличие известных и потенциальных уязвимостей в используемых технологиях и протоколах, особенности обслуживающего персонала АСУТП.

Ключевые механизмы обеспечения ИБ АСУТП с технической точки зрения приводятся ниже.

1. Организация архитектуры межсетевых взаимодействий между технологической и корпоративной сетями. Для решения проблемы часто существуют рекомендации от производителей сетевой инфраструктуры и контроллеров, например, Converged Plantwide Ethernet (CPwE) Design and Implementation Guide (Cisco and Rockwell Automation, Document Reference Number: ENET-TD001E-EN-P). Так как в АСУТП зачастую не применяются последние обновления ПО (системного, прикладного, прошивок контроллеров и т. п.), самым действенным способом защитить компоненты АСУТП является ограничение или полный запрет сетевого доступа к нему из относительно недоверенной сети. При этом возможны различные сетевые архитектуры, например:

a. физическое отделение технологической сети от корпоративной сети, построение независимых резервированных линий связи. Создание демилитаризованной зоны, в которой размещаются промежуточные серверы (транзитный исторический сервер или интерфейс MES, серверы обновлений антивируса, прикладного ПО и ОС и т. д.). Взаимодействие с корпоративной сетью ограничивается с помощью межсетевого экрана. В демилитаризованной зоне может располагаться терминальный сервер, на котором публикуются приложения для удаленной работы, возможны различные технологии реализации данного подхода;

b. гальваническая развязка между корпоративной и технологической сетями, при этом возможно однонаправленное взаимодействие с применением однонаправленных шлюзов.

2. Обеспечение безопасности компонентов АСУТП, в том числе ПЛК, человеко-машинных интерфейсов (применение специализированных защищенных операционных систем, контроль целостности ПО и т. п.)

3. Применение дополнительных подсистем ИБ, обеспечивающих защищенное межсетевое взаимодействие технологической и корпоративной сетей, защиту от подключения несанкционированных устройств в технологических сетях, авторизацию и защиту от перехвата информации при удаленном доступе, обнаружение сетевых вторжений в сеть АСУТП, управление конфигурациями сетевых устройств, централизованный сбор и анализ событий безопасности, анализ защищенности компонент АСУТП, антивирусную защиту сети АСУТП, поведенческий анализ и контроль трафика технологических сетей.

Для снижения рисков применяются и организационные меры защиты, в том числе контроль доступа, обеспечение безопасности паролей, носителей информации, контроль конфигураций, реагирование на инциденты ИБ АСУТП и другие меры.

Заключение

Для безопасного и стабильного функционирования практически любого современного производства необходим комплексный подход к обеспечению ИБ функционирующих АСУТП. В связи с повышенной степенью опасности производств, имеющей место в ряде отраслей промышленности, защита АСУТП от киберугроз является еще и важной задачей государства как гаранта безопасности своих граждан.

На данный момент существуют достаточно глубоко проработанные отечественные и международные методики по защите АСУТП, имеется существенный опыт реализации проектов по обеспечению ИБ АСУТП в отечественной промышленности, накоплены наработки решений, наилучшим образом подходящих для разных ее отраслей.

Однако существуют проблемы, связанные с отсутствием единых законодательных требований к обеспечению ИБ АСУТП. Остается надеяться на то, что эти требования в скором времени будут разработаны, что позволит отечественным предприятиям в полной мере противостоять современным и потенциальным киберугрозам.

Список литературы

1. *Chee-Wooi Ten, Chen-Ching Liu, Manimaran Govindarasu.* Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees // IEEE Transactions On Power Systems. V. 23, N. 4, November. 2008.
2. *Donald L Buckshaw, Gregory S Parnell, Willard L Ulkenholz, Donald L Parks, James M Wallner, O. Sami Saydjari.* Mission Oriented Design Analysis of Critical Information Systems//Military Operations Research. 2005.V10. N2.

Бадеха Иван Александрович *– руководитель направления Департамента информационной безопасности ЗАО «Ай-Теко».*
Контактный телефон 7 (495) 777-10-95.
E-mail: badeha@i-teco.ru
Http://www.i-teco.ru