Актуальные вопросы защиты АСУ ТП и КСИИ

14 февраля на площадке ФГУП «ЦНИИ «Центр» (Москва) прошел семинар-совещание «Актуальные вопросы информационной безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов», организованный Издательским домом «Connect!» в рамках ежегодной серии мероприятий Connect Conferences.
Провели заседание Виктор Гаврилов, советник директора ИПИ РАН, Сергей Новиков, советник генерального директора ИД «CONNECT!», и Сергей Гарбук, советник генерального директора НИИ СУ. Приветствие участникам семинара-совещания направил Игорь Шеремет, член Военно-промышленной комиссии при Правительстве РФ.
Первая часть заседания состояла из серии докладов, посвященных защите АСУ ТП и КСИИ, а также более широкому кругу вопросов информационной безопасности. Вторая часть семинара-совещания проходила в формате круглого стола.

Теория и практика

Состояние вопроса: анализ

Юрий Язов, главный научный сотрудник ГНИИИ ПТЗИ ФСТЭК России, посвятил свой доклад методологическим аспектам анализа рисков нарушения безопасности информации в АСУ ТП критически важных объектов (КВО). Докладчик рассмотрел четыре группы связанных с этим задач. Первая – создание отечественной базы данных уязвимостей программного и аппаратного обеспечения АСУ ТП КВО. Сегодня такие базы данных ведутся только за рубежом. Они крайне слабо структурированы, а существующие форматы описания уязвимостей имеют целый ряд недостатков, например не увязывают уязвимости с угрозами безопасности информации и последствиями их реализации.

Юрий Язов, главный научный сотрудник ГНИИИ ПТЗИ ФСТЭК России

Создание отечественной базы уязвимостей обусловливает необходимость развертывания крупного полигона экспериментальных исследований.

Вторая группа задач связана с оценкой рисков. Понятие риска включает два аспекта: вероятный ущерб и возможность реализации угрозы. При оценке возможности реализации угроз зачастую не учитывается фактор времени. В ряде случаев учет этого фактора позволяет исключить угрозы из числа актуальных.

Третья – прогнозирование последствий реализации угроз. Последствия могут быть материальные, экономические, экологические и пр. Для оценки последствий нужно суммировать все виды ущерба. Это диктует необходимость создания универсальных шкал оценок ущерба в различных сферах деятельности.

Наконец, нужно оценить возможности парирования угроз безопасности информации имеющимися средствами. Сегодня такая оценка выполняется экспертами (и результат зависит от их квалификации) и либо основана на бинарном подходе (парируется/не парируется угроза), либо на проверке соответствия

Игорь Смирнов, Министерство энергетики Российской Федерации


Виктор Гаврилов, ИПИ РАН

состава средств защиты требованиям нормативных документов, при этом не учитывается эффективность применяемых средств защиты.

Игорь Смирнов, консультант отдела безопасности, режима и государственной тайны Министерства энергетики Российской Федерации, рассказал о работах в области безопасности информационных систем, которые ведутся в Минэнерго. Министерством выявлены объекты защиты (виды конфиденциальной информации, информационных систем, используемых программных и технических средств), создана модель угроз, проанализированы различные группы угроз. На основании этого Минэнерго формирует политику информационной безопасности, которая определяет порядок и правила проведения мероприятий по обеспечению ИБ. Политика ИБ включает в себя набор регламентов работы с информацией, использования и защиты информационных систем. В каждом регламенте определяются порядок доступа к объектам защиты, требования к подсистемам управления доступом, обязанности и ответственность должностных лиц.

Отдельно темой АСУ ТП Минэнерго сегодня не занимается. По словам докладчика, информация технологического характера, которая обрабатывается в АСУ ТП, тоже является охраняемой. Но степень ее защиты определяет владелец информации.

Представители НТЦ «Станкоинформзащита» – директор научно-технических программ Сергей Гарбук и заместитель директора департамента АСУ ТП Александр Бурцев сообщили о результатах исследования доступности компонентов АСУ ТП в российском сегменте сети Интернет и степени их уязвимости.

Угрозы для АСУ ТП представляют компьютерные вирусы, хакерские атаки, сбои программного обеспечения, DoS-атаки. Подавляющее большинство программируемых логических контроллеров (ПЛК) имеют не только программные уязвимости, но и глобальные недостатки архитектуры, которые невозможно устранить без обновления парка оборудования и ПО. Основные недостатки присутствующих на рынке ПЛК и АСУ ТП таковы: недостаточность мер аутентификации пользователей и компонентов АСУ ТП;

мнение участника

Антон ШИПУЛИН,
руководитель проектов направления информационной безопасности, компания КРОК

Сегодня для АСУ ТП наиболее актуальны угрозы сбоя, отказов и нарушения штатного режима работы промышленных систем, вызванные ошибочными действиями пользователей, случайным доступом посторонних лиц к управлению системами и распространением вирусов и компьютерных червей. Не менее опасны и преднамеренные атаки со стороны внешних злоумышленников.

Уязвимость АСУ обусловлена отсутствием механизмов безопасности в промышленных протоколах и системах by design, небезупречностью программного обеспечения АСУ и его некорректной конфигурацией. Необходимость интеграции с внешними сетями (корпоративными, WAN, Интернет), использование беспроводных сетей и открытых информационных технологий – операционных систем, сетевых протоколов и служб, удаленного доступа – тоже не способствуют безопасности АСУ ТП.

Предотвратить подобные ситуации можно. Для этого необходимо еще на этапе создания автоматизированных систем или их модернизации сформулировать четкие требования по ИБ. Важно регламентировать процессы и распределить обязанности по обеспечению ИБ между службами промышленных организаций.

Сегодня большинство руководителей промышленных предприятий прекрасно осознают необходимость защиты АСУ ТП, но не все знают, как сделать это эффективно. Прежде всего потому, что нет нормативно-правовых документов и утвержденных методических подходов.

Что касается средств защиты, то помимо традиционных средств ИБ на рынке доступны и специализированные решения для промышленных систем и сетей: шлюзы однонаправленной передачи данных, промышленные межсетевые экраны, системы мониторинга событий и обнаружения вторжений, поддерживающие сигнатуры атак на промышленные службы и протоколы, системы пассивного анализа защищенности. Такие решения КРОК использует в проектах по построению систем технологического управления в защищенном исполнении. Для защиты автоматизированных систем советую также обратить внимание на международные стандарты серии ANSI/ISA SP-99, американские NIST SP 800-82, NISTIR 7628, не стоит игнорировать и рекомендации производителей промышленного оборудования и систем.


Дмитрий Конухов, АНО «Центра энергетики и безопасности»

отсутствие надлежащей проверки целостности кода АСУ ТП и средств разработки; широкие возможности удаленного управления при низком уровне защиты от потенциально опасных действий; возможность нарушения функционирования оборудования или ПО АСУ ТП при наличии доступа к промышленной сети связи.

Чтобы защитить АСУ ТП от интернет-угроз, не следует использовать публичные каналы связи для доступа к оборудованию и ПО АСУ ТП либо нужно надежно защищать их с применением VPN или иных технологий; открытые радиоканалы должны приравниваться к публичным. Следует минимизировать количество логических связей между промышленным сегментом сети и остальным предприятием, обеспечить максимальную изоляцию промышленного сегмента сети от других сегментов сети и Интернета.

Анализ современных угроз объектам критической инфраструктуры сделал **Дмитрий Конухов, научный сотрудник АНО «Центра энергетики и безопасности»**. Исследование инцидентов с вирусом Stuxnet и его «собратьями» (Duqu, Flame, Gauss) заставляет предполагать, что атаки на объекты критической инфраструктуры с помощью вирусов могут быть актами государственного терроризма. Необходимо создание международной конвенции, которая смогла бы регулировать проблемы кибертерроризма. Сейчас механизмы регулирования киберпространства существуют в основном на национальном уровне. Из международных документов имеется только Европейская конвенция по киберпреступлениям 2001 г. Она не является глобальной, кроме того, некоторые страны, в том числе РФ, не присоединились к ней. Поэтому нужно инициировать выработку универсального международного документа, который позволил бы создать правовые основы для противодействия кибертерроризму.

В контексте нормативных и методологических вопросов информационной безопасности, в частности критически важных систем, стоит отметить выступления, прозвучавшие в рамках круглого стола.

Открыл мероприятие Руслан Гаттаров, член Комитета Совета Федерации по науке, образованию, культуре и информационной политике и председатель комиссии по развитию информационного общества. Он сообщил, что комиссия разрабатывает стратегию национальной кибербезопасности, к участию в этой работе приглашаются все заинтересованные компании и эксперты. Принятие стратегии будет способствовать осознанию государством, бизнесом и обществом важности проблемы. Это должен быть доступный документ, в котором содержатся понятные правила действий ведомств, бизнес-структур и граждан, стремящихся защититься от киберугроз.

По оценке Руслана Гаттарова, стратегия может быть написана до конца года, после чего она будет вынесена на рассмотрение Совета Безопасности. Стратегия – это общий политический документ. Следующим этапом должна стать разработка на его основе внутренних концепций и доктрин конкретных ведомств.

Юрий Тимофеев, заместитель председателя ТК 22 «Информационные технологии», рассказал о состоянии процесса международной стандартизации в области защиты АСУ ТП КВО. Эта тема лишь недавно вошла в работу ISO/МЭК – подкомитета 27 («Методы информационной безопасности»). Пока достаточно развитых методов, вокруг которых можно было бы построить международный стандарт, не найдено. Есть отдельные примеры построения национальных стандартов (в Германии, Великобритании), но универсального документа, охватывающего вопросы защиты систем управления всех КВО в международном пространстве, нет. Тем не менее всю совокупность стандартов по защите информации – а их больше 150 – можно и нужно применять. Например, докладчик обратил внимание на стандарт ГОСТ ИСО/МЭК 15408 («Общие критерии оценки безопасности информационных технологий»).

Состояние вопроса: практика

Доклад **Андрея Кондратенко, начальника отдела ОАО «Системный оператор Единой энергетической системы»**, был посвящен мероприятиям по защите ключевых систем информационной инфраструктуры (КСИИ) СО ЕЭС, которые выполнялись согласно документам ФСТЭК. Документы содержат несколько групп требований: наличие системы


Андрей Кондратенко, ОАО «Системный оператор Единой энергетической системы»


Герман Клочко, ФГУП «Росморпорт»

обнаружения вторжений; системы анализа защищенности (выявления ошибок в конфигурации ПО, уязвимостей в версиях ПО, слабых паролей); антивирусная защита; обеспечение безопасности межсетевого взаимодействия (межсетевые экраны); контроль отсутствия недекларированных возможностей; защита от несанкционированного доступа.

Выводы по опыту работы таковы. Требования ФСТЭК по защите КСИИ понятны, по ним можно работать, но они не всегда выполнимы, следовательно, нуждаются в тщательной адаптации для конкретного предприятия. В организации должны быть собственные специалисты по ИБ, досконально разбирающиеся в вопросах работы АСУ.

Выполнение требований по защите АСУ обходится дорого. Поэтому расчет стоимости обеспечения ИБ должен производиться еще на стадии создания автоматизированной системы. Но этого никогда не происходит, тем более что в эксплуатации находится множество унаследованных систем, которые некому дорабатывать.

Требования ФСТЭК носят рекомендательный характер, обязательных законодательных актов нет. Поэтому сложно объяснить руководству и персоналу, почему необходимо выполнять требования по защите АСУ. Кроме того, требования по защите КСИИ не учитывают особенности АСУ как систем реального времени. Не учитываются в них и тенденции развития ИТ – виртуализация, интеграция систем со службой Active Directory и пр.

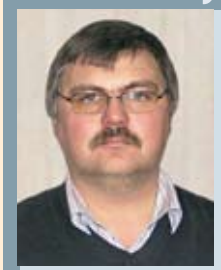
Профессиональному сообществу следует подумать над тем, как сделать стоимость мер по защите АСУ доступной для владельцев бизнеса, а процесс обеспечения ИБ – незаметным для пользователей АСУ. Кроме того, нужны отраслевые стандарты безопасности и орган, который координировал бы работы по обеспечению информационной безопасности АСУ ТП всей энергетической системы страны.

Об организационных аспектах защиты КСИИ систем обеспечения безопасности мореплавания (СОБМ) в портах СЗФО рассказал **Герман Клочко, начальник отдела по защите информации Северо-Западного бассейнового филиала ФГУП «Росморпорт»**.

В частности, речь шла о системе управления движением судов (СУДС). Система была отнесена к КСИИ третьего уровня важности на основании документа Совета Безопасности «Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий».

Деятельность по защите информационных систем, в том числе КСИИ, во всех филиалах координируется на уровне Центрального аппарата «Росморпорта». В свое время

мнение участника



Андрей ПОМЕШКИН,
директор ООО «Системы информационной безопасности»

В России вопрос защиты АСУ ТП, точнее КВО и КСИИ, начал обостряться еще до появления Stuxnet. Документы ФСТЭК появились не на пустом месте, серьезным стимулом стала авария на Саяно-Шушенской ГЭС в августе 2009 г. Можно выделить две независимые, но традиционно связанные темы, касающиеся объектов КВО: защита технологических сетей и защита критически важных информационных систем (например, сайта государственного органа).

Основные угрозы безопасности АСУ ТП – угроза остановки объекта управления или отказа в обслуживании. Здесь мы имеем три проблемы.

Первая – возможность внедрения закладок в АСУ ТП (SCADA) иностранного производства. Поэтому требуется изоляция системы от возможного канала получения команды на активацию закладки. Закладки могут внедряться как разработчиком, так и лицами, сопровождающими систему. Последствием может быть полный выход из строя системы управления без возможности замены узлов, поскольку в них та же закладка.

Вторая – угроза нарушения целостности системы как на уровне ПО, так и на уровне оборудования. Наиболее вероятна ее реализация через «трояны» и вирусы класса Stuxnet. Последствия здесь поправимые – линия выходит из строя, но возможны восстановление с чистых носителей и замена узлов.

Третья проблема – угроза нарушения доступности из-за неправильного функционирования СЗИ. В случае ее реализации вопрос решается путем остановки СЗИ.

Основные проблемы защиты АСУ ТП связаны с тем, что это объект, функционирующий в режиме реального времени или близком к нему. Плюс ограничены ресурсы в самой системе – как процессорное время, так и память. Как следствие – нет средств безопасности, гарантирующих временные характеристики.

Нормативная база также нуждается в доработке с учетом современных угроз и особенностей работы АСУ ТП.

Если говорить о существующих в мире практиках защиты SCADA, то на сегодняшний день большая работа ведется в США: по приведению нормативной базы в соответствие современным требованиям и условиям, разработке лучших практик и стандартов. В принципе, мы находимся примерно на одном уровне с точки зрения используемых в SCADA-системах технологических решений – периода середины – конца 80-х гг. прошлого века.

Центральным аппаратом было организовано совещание с участием представителей ФСТЭК и разработчиков информационных систем, в ходе которого регулятора удалось убедить в том, что информация в СУДС носит сервисный характер и не содержит гостайны и другой конфиденциальной информации. После этого были разработаны и согласованы с ФСТЭК модель угроз и техническое задание.

СУДС и другие КСИИ «Росморпорта» (например, Глобальная морская система спасения при бедствии) состоят из множества подсистем. Как объекты, обеспечивающие условия безопасного судоходства в морских портах и на подходах к ним, они защищаются и сертифицируются в соответствии с требованиями профильных организаций, в том числе международных. Отказ одного объекта (подсистемы) может обусловить ухудшение работы системы в целом, но не приводит к выходу ее из строя. Поэтому в соответствии с руководящими документами ФСТЭК «Росморпорт» имеет право защищать только самые важные подсистемы, а не системы целиком.

Существуют проблемы с внедрением разработанных по требованиям ФСТЭК решений по защите КСИИ. В первую очередь это сопротивление разработчиков и эксплуатантов – в отсутствие законодательных мер воздействия они не заинтересованы в выполнении требований, которые выдвигает администрация «Росморпорта». Иногда решения, отработанные на стенде, невозможно внедрить на реальной системе до изменения разработчиком ее программно-аппаратной части.

Тем не менее докладчик считает, что документы ФСТЭК полезны, ими можно пользоваться и в сфере судоходства – если делать это вдумчиво. Он также отметил высокое качество работы подрядчиков – компаний «Информзащита» и «Газинформсервис».

Об основных проблемах, которые возникают в проектах по защите АСУ ТП, рассказал **Алексей Косихин, руководитель направления Центра информационной безопасности компании «Инфосистемы Джет»**. Чтобы получить адекватное представление о защищенности объекта, требуется обследование, которое в случае территориальной распределенности объектов или большого количества АСУ ТП на предприятии может затянуться. Квалификация персонала на местах тоже оставляет желать лучшего. Подчас сами пользователи не понимают до конца, как работает конкретная АСУ ТП, особенно унаследованная.

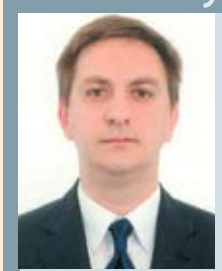

Алексей Косихин, компания «Инфосистемы Джет»

Затем возникает проблема внутренних согласований, нередко отнимающих немало времени, за которое успевает измениться инфраструктура предприятия.

На стадии эксплуатации проблемы чаще всего связаны с ограниченным штатом специалистов по безопасности у заказчика и недостатком у них опыта. Внутри компании-заказчика далеко не всегда выполняются регламенты, разработанные подрядчиком. Поэтому в компании «Инфосистемы Джет» было организовано сервисное подразделение, которое обеспечит заказчика необходимыми ресурсами для эксплуатации и поддержания в актуальном состоянии решений по ИБ, позволит воспользоваться опытом диагностики и устранения проблем, а также даст определенные гарантии в виде прописанных штрафов за несоблюдение SLA.

Алексей Мальнев, начальник отдела защиты КСИИ компании «АМТ Груп», представил решения для защиты ЛВС АСУ ТП. Идеальным вариантом была бы полная изоляция АСУ ТП, но на практике такой подход неприемлем.

мнение участника



Виктор БУЙНАК,
руководитель направления, отдел развития бизнеса, ОАО «ИнфоТеКС»

Среди угроз информационной безопасности АСУ ТП выделяют три класса: техногенные, антропогенные и несанкционированного доступа. Угроза несанкционированного доступа является актуальной, поскольку между АСУ ТП и ЛВС предприятия происходит интенсивный информационный обмен.

Поэтому критически важны меры по формированию выделенных защищенных VPN-сетей, защищенных технологических сетей передачи данных и использование средств защиты периметра, межсетевого экранирования, обнаружения вторжений (IDS), криптографической защиты каналов связи.

Вопросы защиты АСУ ТП успешно решаются с помощью продуктовой линейки ViPNet производства ОАО «ИнфоТеКС». Комплекс ViPNet Custom позволяет создать для АСУ ТП защищенную среду передачи данных, систем телеметрии, датчиков, аудио- и видеосвязи с использованием проводных и беспроводных каналов. Безопасность информации, передаваемой компонентами АСУ ТП при организации обмена как по выделенным каналам, так и через сеть Интернет, обеспечивается применением сертифицированных межсетевых экранов и криптографических средств защиты информации ViPNet, выполняющих функции прозрачного шифрования протокола IP.

Технология ViPNet позволяет обеспечить защищенное удаленное обновление версий ПО, справочников доступа и ключей рабочих станций виртуальной сети. Указанное свойство существенно упрощает процесс модернизации и конфигурирования сети и уменьшает расходы по ее обслуживанию.

Однако помимо технологий есть еще организационные и кадровые вопросы. Персонал, ответственный за поддержку АСУ ТП, обычно хорошо разбирается в проблемах физической безопасности на производстве, но совершенно не знаком с рисками, целями и задачами ИБ АСУ ТП.

Существует также проблема недостаточности нормативной базы: нет четких, прозрачных, непротиворечивых требований к ИБ АСУ ТП. Зачастую в технических требованиях по разработке систем отсутствуют требования по защите информации, которые учитывались бы разработчиками, – сигнализация о попытках нарушения защиты, контроль доступа к подсистемам АСУ ТП, каналам связи, технологическим объектам управления, узлам сети и пр.


Алексей Мальнев, компания «АМТ-ГРУП»

Альтернативный сценарий – использование на периметре ЛВС АСУ ТП межсетевого экрана (МСЭ), а лучше двух. При этом между корпоративной сетью и АСУ ТП может формироваться одна (или несколько) демилитаризованная зона (DMZ).

Более защищенный сценарий предусматривает исключение прямых сессий между корпоративной сетью и АСУ ТП. Для такого случая в DMZ ставится терминальный сервер.

Иногда регуляторы требуют полной изоляции АСУ ТП. В подобных ситуациях предлагается технология, которая позволяет организовать одностороннее межсетевое взаимодействие – либо с прямым контуром, либо с двусторонне направленным. Одно из таких решений – программно-аппаратный комплекс Fox-IT DataDiode. Комплекс включает в себя два прокси-сервера – доверенный и недоверенный. Сигнал от ЛВС АСУ ТП принимается доверенным прокси, далее поступает на устройство аппаратной организации одностороннего обмена, затем на недоверенный прокси, откуда передается во внешнюю сеть. Такая схема позволяет решать различные задачи. Например, создавать зеркало SCADA Historian & Reporting Server в корпоративном сегменте. При помощи обратного контура можно реализовать периодическую закачку данных (например, обновлений) внутрь сети АСУ ТП.

Если говорить о внутренней структуре ЛВС АСУ ТП, то в защите нуждаются в первую очередь верхний и средний уровни (уровень управления и уровень контроллеров). Внутри ЛВС АСУ ТП, в отличие от периметра, важно использовать специализированные средства защиты. Например, промышленный МСЭ Tofinosecurity производства компании Belden, который предлагается ставить между верхним и средним уровнями.

Андрей Духвалов, стратег по развитию технологий «Лаборатории Касперского», рассказал о решении по защите АСУ ТП, над которым работает компания. Как показывают исследования, уязвимы все компоненты АСУ ТП – контроллеры (ПЛК), ПО АСУ ТП, протоколы связи в технологической сети. Кроме того, необходимо обеспечивать информационную безопасность на стыке офисной и технологической сетей и контролировать работу персонала. Ни одному из компонентов невозможно доверять. Значит, в АСУ ТП нужно ввести доверенный элемент, способный контролировать поведение всех остальных. С точки зрения «Лаборатории Касперского» таковым должна стать безопасная операционная система. Операционная система для АСУ ТП, которую


Андрей Духвалов, «Лаборатория Касперского»

компания разрабатывает с нуля, имеет микроядерную архитектуру. Все приложения, в том числе системные, состоят из верифицируемых модулей. Прямые связи между программными модулями не допускаются. Каждый из них может получить сервис от другого модуля лишь посредством ядра ОС, которое проверяет соответствие запроса на сервис заданному сценарию. Таким образом исключается исполнение незаявленного функционала. Найдены простые и

мнение участника

Николай НАШИВОЧНИКОВ,
заместитель генерального директора – технический директор ООО «Газинформсервис»

Основная проблема защиты АСУ ТП заключается в том, что требования систем безопасности могут влиять на архитектуру самой АСУ ТП и выбор конкретных средств. Поэтому важно привлекать специалистов по ИБ на самом раннем этапе – при формулировании требований к АСУ ТП. Проектирование системы безопасности должно вестись уже после окончания проектирования самой АСУ ТП и фиксации применяемых в ней решений. Увы, это выполняется не всегда, и по факту решения могут не учитывать последних изменений, что приводит к ряду проблем как при вводе систем в действие, так и в процессе их эксплуатации.

Другой проблемой является недостаток нормативных правовых актов, определяющих требования по обеспечению ИБ в АСУ ТП. Требования в действующих документах привязываются к той или иной классификации объекта, которая не всегда бывает произведена. Например, документ ФСТЭК России «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» привязывается к уровню важности системы. Многие организации испытывают объективные сложности с классификацией своих систем и определением уровня их важности.

Часть проблем, связанных с обеспечением ИБ в АСУ ТП (например, долгий срок жизни системы, ограниченная возможность оперативных обновлений), вполне объективна и не может быть решена. Другая часть (например, выпуск обновлений специализированного ПО) не может быть решена силами эксплуатирующих организаций и разработчиков систем безопасности – требуются усилия производителей специализированного ПО и оборудования.

В ряде компаний приняты стандарты организации и рекомендации. Например, документы ОАО «Газпром» серии 4.2 дают хорошую базу для построения систем безопасности АСУ ТП. Однако они не являются обязательными для всех.

Начинают появляться специализированные решения по защите АСУ ТП от различных производителей, однако область эта сравнительно молода и явные фавориты пока не просматриваются.

надежные средства описания корректных сценариев поведения любого программного модуля.

В зону действия безопасной ОС «Лаборатория Касперского» предлагает включить прежде всего ПЛК – она позволит контролировать их взаимодействие с другими узлами АСУ ТП посредством доверенных фильтров. Постепенно систему фильтрации можно распространять на остальные компоненты АСУ ТП. Для фильтров можно выбирать активный или пассивный режим, при этом вся их совокупность составит своего рода систему мониторинга, которая позволит получать общую картину состояния АСУ ТП.

Дискуссия об актуальном

В фокусе — нормативная база

С самого начала дискуссии выявилась потребность определиться с понятиями и терминологией. Понятие «информационная безопасность» очень широкое: оно включает и защиту персональных данных граждан, и вопросы фильтрации контента, и кибербезопасность как защиту информации в системах, работающих на базе компьютерных технологий. В последнем случае информация может быть составляющей гостайну, конфиденциальной, технологической. Применительно к АСУ ТП речь идет преимущественно о технологической информации, состояние которой влияет на функциональную безопасность объекта.

В атомной отрасли понятие «информационная безопасность» вообще не используется, есть понятие «ядерная безопасность», о чем напомнил **Андрей Загородный, ведущий специалист центра 920-го отделения АСУ ТП ВНИИАЭС**. Документ ОПБ-88/97 определяет ранжирование элементов (систем) атомной станции по четырем категориям в соответствии со значимостью последствий их отказа. Причем имеются в виду АСУ ТП, функциональные элементы АЭС. Есть ли смысл вести речь отдельно о защите АСУ ТП? «Атомщики» говорят о двух типах негативных последствий: нарушении мощности станции и радиационной опасности. Не важно, по вине какого из элементов такие последствия наступают, подход к обеспечению безопасности ядерного объекта должен быть комплексным.

В каждой отрасли существует своя специфика задач обеспечения безопасности. И эти задачи следует решать на уровне конкретной отрасли. Требования информационной безопасности обязаны выполнять предприятия всех отраслей, но в положениях федеральных законов, касающихся конкретных отраслей, эти требования должны быть определены более четко.

В сфере энергетики, как считает **Алексей Данилов, заместитель начальника департамента информационной безопасности и специальных проектов ФСК ЕЭС**, необходимо согласовать законодательную и нормативную базы. Федеральный закон № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» говорит о КВО ТЭК. Статья 11 касается безопасности информационных систем объектов ТЭК, подзаконные акты – исключительно защиты объектов ТЭК, но не детализируют подход к категорированию и защите информационных систем. Кроме того, нормативные документы фактически отдают категорирование автоматизированных систем на откуп их владельцам, что неправильно. Владелец может просто не понимать, что его система критически важная. Целесообразно создать коллегиальный орган, который бы принимал решение о категорировании АСУ. Либо результаты категорирования объектов должны автоматически распространяться на имеющиеся на этих объектах автоматизированные системы (если объект критически важный, то и его АСУ ТП относится к той же категории).

Энергетическая система страны представляет собой множество взаимосвязанных субъектов хозяйственной деятельности. По мнению Алексея Данилова, должна существовать единая политика в сфере

мнение участника

Руслан СТЕФАНОВ,
руководитель направления защиты АСУ ТП,
ОАО «ЭЛВИС-ПЛЮС»

В настоящее время наиболее актуальны угрозы целенаправленных внешних информационных воздействий на АСУ ТП. Это связано с взаимодействием АСУ ТП территориально разнесенных объектов и усиливающейся интеграцией с другими корпоративными системами. Основным источником таких угроз становятся злоумышленники, целью которых является нанесение ущерба активам предприятия и инфраструктуре государства. Эти угрозы носят глобальный характер и могут нанести вред как отдельному государству, так и всему миру.

Другой угрозой, которой также необходимо уделять внимание, является некачественное программное обеспечение АСУ ТП – как прикладное, так и системное. Исходя из значительных сложностей обновления такого ПО в процессе его эксплуатации, необходимо внедрять методы безопасного кодирования (программирования), поиска ошибок, контроля цепочки поставок на начальных этапах его жизненного цикла. Другим путем решения проблемы является разработка технологий гарантированно безопасного обновления. Например, американский департамент энергетики (DOE) выделил одно из главных направлений развития технологий: разработку методов формальной верификации, которые обеспечат детерминированность процессов обновления ПО или использования патчей. Благодаря применению этих технологий процессы будут выполнены именно так, как задумано, при этом они не смогут оказать никаких неожиданных воздействий или скомпрометировать систему.

Основная проблема защиты АСУ ТП связана с конфликтом между информационной и промышленной (функциональной) безопасностью. Промышленная безопасность хорошо нейтрализует многие угрозы естественного происхождения: случайные ошибки персонала, природные и т. п. Однако против целенаправленных угроз ее методы недостаточно эффективны. Поэтому для защиты АСУ ТП должны использоваться методы информационной безопасности.

Реальность такова, что все попытки «быстро повысить» информационную безопасность АСУ ТП будут разбиваться о консервативность промышленных систем, в которые с самого начала заложены требования надежности и промышленной безопасности. И это нормально с учетом того, что самые необходимые меры информационной безопасности все же постепенно внедряются в продукты и решения по автоматизации технологических процессов.

организации взаимосвязей между ними, построения корпоративного и технологического сегментов сети. Для этого требуются отраслевые стандарты (создание которых могло бы взять на себя, например, Минэнерго). За основу можно принять лучшие практики, зарубежные отраслевые стандарты, с внесением в них изменений с учетом национальной специфики.

Валерий Омаров, главный специалист «Газпром энергохолдинга», считает, что по логике № 256-ФЗ и ст. 11 существующая нормативная база по ИБ достаточна и ею надо пользоваться. Однако нормативная база определяет информацию о системах защиты информации АСУ ТП как информацию ограниченного доступа и не дает ответа на вопрос, какую информацию в АСУ ТП необходимо защищать и каковы классы (категории) ее защиты. Необходимы подзаконные акты, определяющие информацию, которая должна защищаться в АСУ ТП, а также понятия и правила, в том числе требования к персоналу, требования к самой АСУ ТП по обеспечению ИБ, которые должны выполнять разработчики АСУ ТП.

По поводу того, нужно ли категорировать технологическую информацию, находящуюся в АСУ ТП, мнения разделились. С одной стороны, если число категорий будет совпадать с количеством классов защиты, которые определены руководящими документами, это позволит использовать имеющуюся нормативную базу. С другой – не вся ли технологическая информация одинакова и равнозначна? Возможно, нет: например, воздействие на сигналы телеуправления и сигналы телеметрии могут иметь разные последствия. Хотя с этим утверждением не все согласны.

Категорировать информацию в АСУТП безотносительно системы не имеет смысла, считает **Юрий Язов**. Можно лишь выделить критически важную информацию в системе. Впоследствии ее целесообразно делить по категориям в зависимости от последствий воздействия на АСУТП, оцениваемых по универсальным шкалам. В свою очередь, **Евгений Яковлев, советник Департамента защиты государственной тайны и информации Госкорпорации «Росатом»**, заметил, что он готов согласиться с таким подходом, если речь идет о построении отдельных систем. Но поскольку все системы объекта связаны, более слабая защита какой-то из них создает потенциальные уязвимости.

Руководство к действию — документы по КСИИ?

В существующих руководящих документах ФСТЭК России по КСИИ от 2007 г., как отметил **Юрий Язов**, в отличие от руководящих документов по АС и СВТ, ведется речь не о конфиденциальной информации, а о технологической. Эти документы нуждаются в переработке, в частности, с учетом опыта проверяющих специалистов и отраслевой специфики систем. Такая работа будет вестись.

Определить, относятся ли информационные системы к КСИИ, позволяет документ Совета Безопасности от 2005 г. «Система признаков критически важных объектов…» (документ опять же закрытый). Им воспользовались в СО ЕЭС. **Александр Зализный, ведущий эксперт СО ЕЭС**, считает, что заложенная в документе система критериев вполне достаточна, в том числе для энергетики. Однако сертифицированные средства защиты существуют только для информации ограниченного доступа, а средств защиты АСУ ТП, работающих в режиме реального времени, нет. Предприятие, выполняющее нормативные требования, сталкивается с риском отказа сертифицированного средства.

Документ по системе признаков и критериев тоже нуждается в доработке, согласен **Юрий Язов**. Но дело это долгое и непростое, тем более что в соответствии с ним ведется реестр ключевых систем информационной инфраструктуры.

Что касается реестра, то, по словам представителя ФСТЭК, он пополняется ежегодно, а перечни ключевых систем предоставляют профильные министерства. Однако некоторые участники обсуждения усомнились в том, что механизм поддержки актуальности реестра работает адекватно. Например, представителям СО ЕЭС не удается

мнение участника

Елизавета СПАСЕННЫХ,
менеджер по развитию бизнеса,
компания «Информзащита»

Для предприятий особую актуальность имеют угрозы, связанные с несанкционированным доступом к элементам АСУ ТП. При этом не столь важно, как были получены привилегии доступа – путем внешнего информационного воздействия или внутреннего. Необходимо минимизировать влияние человеческого фактора и создать комплексную систему защиты информации, включающую как технические, так и организационные меры.

Исторически АСУ ТП развивались как изолированные системы, работающие по специализированным протоколам. К тому же они находились вне зоны контроля подразделений, ответственных за ИБ. Одна из тенденций последних лет – переход АСУ ТП на более распространенные технологии обработки информации. Другая тенденция – объединение технологических и корпоративных сетей, вследствие чего ответственность за обеспечение безопасности передается людям, которые прежде не имели отношения к защите технологических сетей. Однако существующие подходы к защите корпоративных сетей часто неприменимы из-за особенностей АСУ ТП или выполняемых с ее помощью бизнес-процессов. Проблема определения подхода к созданию комплексной системы защиты выходит на новый уровень – от специалистов требуется предметное знание не только вопросов информационной безопасности, но и технологических процессов.

Есть и другие факторы, которые негативно сказываются на обеспечении комплексной защиты. Это и небольшой выбор средств технической защиты, и риски лишиться технической поддержки со стороны разработчика АСУ ТП, и недостаточность понимания персоналом важности соблюдения мер безопасности, и отсутствие прямой заинтересованности руководства во внедрении мер защиты.

Сегодня многие компании разрабатывают собственные требования к защите АСУ ТП. На текущий момент такой подход является оптимальным, потому что каждая АСУ ТП имеет индивидуальные особенности, которые необходимо учитывать. Использование международных отраслевых стандартов является хорошей практикой, однако это не панацея. Самостоятельная разработка требований к ИБ позволяет учесть все необходимые нюансы.

получить однозначную информацию о том, какие объекты относятся к КСИИ и подлежат проверке со стороны регулятора.

Герман Клочко, начальник отдела по защите информации СЗБФ ФГУП «Росморпорт», рассказал об организационных аспектах обеспечения безопасности информации в системах обеспечения безопасности мореплавания в портах СЗФО, отнесенных к КСИИ, и возможности выполнения требований регулятора к объектам КСИИ, с обязательным учетом особенностей их построения, специфики функционирования и территориального расположения.

Докладчик отметил, что предприятию, имеющему объекты транспортной инфраструктуры, приходится иметь дело с требованиями МЧС, транспортной безопасности, ФСТЭК, в частности по обеспечению безопасности и категорированию объектов. Все документы сочетаются между собой, но зачастую дублируют друг друга и не имели единых критериев при их разработке. К сожалению, отсутствуют необходимые нормативные акты по обеспечению безопасности информации в КСИИ. Существующие документы, утвержденные заместителем директора ФСТЭК от 2008 г., носят рекомендательный характер, но безусловно полезны, на их основе возможно обеспечение безопасности информации в КСИИ, в том числе и в области обеспечения безопасности мореплавания.

Нужен испытательный полигон

Александр Кархов, начальник службы информатизации Дирекции железнодорожных вокзалов – филиала ОАО «РЖД», обратил внимание еще на один аспект защиты АСУ, который практически не отражен в нормативной базе: современная система представляет собой распределенный вычислительный комплекс, в нем помимо информации


Александр Кархов, ОАО «РЖД»

как таковой существуют еще протоколы и алгоритмы работы с ней. Вмешательство или заложенные в них уязвимости могут иметь самые серьезные последствия.

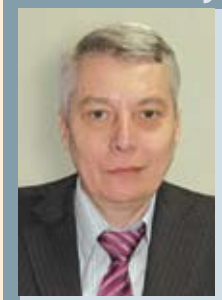
Эта реплика вернула обсуждение к понятию функциональной безопасности. Нормативные документы ФСБ и ФСТЭК касаются защиты информации с точки зрения целостности, доступности, конфиденциальности, но полностью понятия функциональной безопасности не покрывают. Между тем если не регулировать данный аспект, полноценная защита обеспечиваться не будет.

Таким образом, необходимы нормативные документы, оперирующие понятием «функциональная безопасность» применительно к информационным системам. Но кто должен их выпускать? И кто сможет проверять ту же корректность работы алгоритмов? В частности, **Александр Максимовский, заместитель начальника Управления ФСБ России**, отметил, что это не в компетенции ФСБ и ФСТЭК, хотя бы потому, что такая работа требует глубокого понимания технологий АСУ ТП.

Юрий Язов напомнил об американском опыте: в 2005 г. в США был создан мощный испытательный центр, куда все структуры – операторы КВО направляют ПО на экспертизу.

Идея испытательного центра вызвала интерес, тем более что структуры, имеющие в своем распоряжении множество объектов (в частности, ФСК ЕЭС), заинтересованы в том, чтобы у них не было

мнение участника



Сергей АКИМОВ,
советник генерального директора по работе с регулирующими органами, государственными и общественными организациями, директор департамента аттестации и лицензионной работы, компания LETA

Информация в АСУ ТП в отличие от других информационных систем имеет прямую взаимосвязь с физическим объектом, например через систему установленных на нем датчиков и исполнительных механизмов. Любое воздействие на них может привести к негативным последствиям. Злоумышленники могут применять для этого все виды известных средств: компьютерные вирусы, хакерские атаки, сбои ПО, DoS-атаки. Актуальны и угрозы со стороны возможного инсайдера. В результату, как минимум, – убытки от остановки производства, как максимум, – техногенная катастрофа.

К сожалению, в России предпосылок для этого довольно много, и прежде всего они связаны с недостаточностью нормативной правовой базы, отсутствием единой государственной системы контроля состояния безопасности информационно-телекоммуникационных систем, недостатком специализированных технических средств, в отдельных случаях – с непониманием бизнес-подразделениями важности задачи защиты АСУ ТП. Проблемой являются и недостаток квалифицированных «безопасников», отсутствие четких методических материалов, например в виде отраслевых рекомендаций.

В США часть организаций под эгидой US-CERT серьезно озаботилась проблемой защиты промышленных объектов (в нашем случае – КВО) и выпустила ряд методических рекомендаций, нормативных документов. А что сделано в России? Совершенствуется нормативная база, Президентом РФ утверждены «Направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации», обсуждается проект федерального закона, который отразил бы особенности обеспечения ИБ критически важных объектов и позволил бы упорядочить отношения между государственными органами и субъектами информационной и телекоммуникационной инфраструктуры.

Но нормативного обеспечения работ явно недостаточно. Требуются консолидированные усилия всех сторон – интеграторов и вендоров (которые сегодня, к сожалению, занимают выжидательную позицию), профильных ассоциаций, которые могли бы облегчить жизнь предприятиям, эксплуатирующим АСУ ТП, например озаботившись выпуском внятных отраслевых рекомендаций и методик проведения работ.

«зоопарка», но имелась бы возможность распространять на объектах сертифицированные системы. Кроме того, испытательный полигон позволит апробировать различные методы защиты АСУ ТП.

Создание испытательного стенда – затратная и трудоемкая работа. На какой базе и за чей счет ее выполнять?

Как сообщил **Валерий Бордюже, председатель Координационного Совета по информационным технологиям предприятий оборонно-промышленного комплекса РФ**, подобный центр создают сейчас предприятия ОПК на базе ФГУП ВИМИ. Тестировать предполагается ПО систем управления предприятием и системы MES, САПР, CAD/CAM. Что касается АСУ ТП, то, поскольку они имеют отраслевую специфику, целесообразно создавать испытательные стенды в каждой отрасли.

Многие участники круглого стола поддержали эту идею. Однако, например, **Андрей Духвалов** полагает, что, несмотря на различие в технологических процессах отраслей и разные последствия их нарушения, везде используется один и тот же набор контроллеров. Поэтому испытательная площадка может быть единой, но в ее работе должны принимать участие представители всех заинтересованных отраслей. Он также отметил, что «Лаборатория Касперского» заинтересована в создании центра тестирования и готова участвовать в этой работе.

Идею единой испытательной площадки поддержал **Александр Кархов**. Конечно, протестировать устойчивость системы управления объектом в целом можно только с учетом отраслевых особенностей. Но, например, у контроллера две стороны: одна («информационная») смотрит в систему управления, другая – собственно на технологический процесс (непосредственно измерительные и управляющие устройства). Причем «информационная» часть контроллеров – типовая для разных отраслей и применений. В этой части разных контроллеров не так много. Централизованно можно проверить безопасность «информационной» части контроллеров, это снимет большую часть проблем, поскольку именно «информационная» часть контроллера подвергается

Руслан Гаттаров, член Комитета Совета Федерации по науке, образованию, культуре и информационной политике и председатель комиссии по развитию информационного общества (справа)

атакам. Как это организовать? Предлагаемая мера спорная, но, на взгляд спикера, единственно реальная. Если ввести систему обязательной сертификации оборудования и ПО, у производителей появится стимул проводить такую сертификацию и финансировать соответствующие работы, иногда – готовность передавать исходные коды управляющего ПО. В этом случае центр может быть создан без государственных вливаний.

Вопросы финансирования

Вопросы финансирования актуальны не только для создания испытательного стенда, но и для реализации оператором технических мер защиты критически важных систем. По мнению **Андрея Кондратенко**, следует централизованно оценить стоимость каждого профиля защиты. Это помешает некоторым интеграторам «заламывать цены», даст ориентиры специалистам предприятий и позволит обосновать стоимость мер защиты перед руководством.

С точки зрения представителей энергетической отрасли, регулирование и финансирование информационной безопасности КВО ТЭК – вещи связанные. В конечном счете затраты закладываются в тарифы. Значит, должна существовать государственная целевая программа, включающая и вопросы категорирования объектов ТЭК, и вопросы финансирования их защиты. Тем более что объекты энергетического комплекса – это объекты государственного значения.

Сергей Гарбук высказал следующую идею: защищаемую технологическую информацию нужно разделить на два вида – информация, которая должна защищаться в силу ее государственной значимости (аналог гостайны), и информация, защищаемая опционально (аналог коммерческой тайны). Если информация отнесена к первому виду, то защищать ее надлежит в обязательном порядке. Что касается информации второго вида, то операторы могут найти способы сбалансированной оценки последствий ее нарушения и рационального объема затрат. При этом необходимо стандартизировать правила отнесения информации к категории государственно значимой.

Валерий Бордюже предложил рассмотреть другой путь. Есть бюджет предприятий, который выделяется на ИКТ. Руководящие структуры могли бы предписать использовать часть этого бюджета целевым назначением – на финансирование работ по информационной безопасности.

По итогам обсуждения участники семинара-совещания приняли резолюцию, которая была направлена в Совет Безопасности Российской Федерации. ■

РЕЗОЛЮЦИЯ

Семинара-совещания

«Актуальные вопросы информационной безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов»

14 февраль 2013 г.

ФГУП «ЦНИИ «Центр», г. Москва

г. Москва, ул. Садовая-Кудринская, д. 11, стр. 1

Организатор
Издательство «CONNECT!»

ПРИНИМАЯ ВО ВНИМАНИЕ, что реализация основных направлений государственной политики (ОНГП) в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами (АСУ ТП) критически важных объектов (КВО) инфраструктуры Российской Федерации требует решения вопросов обеспечения информационной безопасности (ИБ АСУ ТП КВО), совершенствования нормативно-правового регулирования, координации работ со стороны регуляторов, владельцев КВО и поставщиков средств ИБ-технологий, а также разработки технологий их проведения, участники семинара-совещания полагают целесообразным:

1. При разработке нормативных правовых документов, предусмотренных ОНГП:

1.1. уточнить понятийный аппарат, исключив неоднозначное толкование определений: «объект критически важной инфраструктуры Российской Федерации», «автоматизированная система управления производственными и технологическими процессами критически важного объекта инфраструктуры Российской Федерации», «критическая информационная инфраструктура Российской Федерации»;

1.2. определить порядок и полномочия сторон по отнесению АСУ ТП к КВО инфраструктуры Российской Федерации, предусмотрев классификацию этих систем в зависимости от тяжести наступающих последствий;

1.3. определить и наделить полномочиями организации, которые возьмут на себя разработку отраслевых стандартов в области ИБ АСУ ТП КВО, а также их аттестацию по требованиям безопасности информации:

– транспортного комплекса;

– топливно-энергетического комплекса;

– машиностроения и оборонно-промышленного комплекса;

– телекоммуникаций, телевидения и радиовещания и др.;

1.4. доработать нормативную базу в области защиты информации и создания средств защиты информации с учетом особенностей обеспечения информационной безопасности в автоматизированных системах управления технологическими процессами и других автоматизированных системах, осуществляющих обработку информации в реальном масштабе времени с учетом предложений головных организаций по стандартизации оборонно-промышленного комплекса, транспортного комплекса, топливно-энергетического комплекса, а также других заинтересованных отраслей;

1.5. разработать подзаконные акты к № ФЗ-256 от 21.07.2011 «О безопасности объектов топливно-энергетического комплекса» в целях обеспечения безопасности информационных систем объектов топливно-энергетического комплекса в части паспортизации, категорирования информации, формирования и реализации требований;

1.6. определить порядок аккредитации и лицензирования организаций, осуществляющих деятельность по оценке соответствия автоматизированных систем управления технологическими процессами КВО предъявляемым требованиям в области обеспечения информационной безопасности.

2. Обратить особое внимание на необходимость создания Национальной тестовой лаборатории по исследованию проблем информационной безопасности программных и аппаратных средств АСУ ТП применительно к КСИИ КВО с активным участием министерств, ведомств и организаций из заинтересованных отраслей (ТЭК, транспорт, нефтехимия, водоснабжение и т.д.).

3. Участники семинара-совещания благодарны журналу CONNECT! за инициативу проведения семинара-совещания и предлагают рассмотреть возможность проведения под эгидой Совета Безопасности Российской Федерации Всероссийской конференции по проблемам безопасности информационных и телекоммуникационных систем критически важных объектов, в тематику, которой включить вопросы ИБ АСУ ТП КВО.

4. Участники семинара-совещания с одобрением восприняли резолюцию и рекомендуют направить ее в Аппарат Совета Безопасности Российской Федерации.