

# АСУ ТП КВО: от защиты объекта к безопасности системы

4–5 февраля 2014 г. в Москве в конференц-зале РАНХ и ГС состоялась конференция «Информационная безопасность АСУ ТП КВО», организованная Издательским домом «Connect». Большой интерес к мероприятию проявили представители органов государственной власти, научно-исследовательских институтов, руководители компаний и предприятий разных отраслей, разработчики систем управления, производители и поставщики оборудования, программного обеспечения, специалисты в сфере ИБ. Насыщенная программа, активность участников мероприятия в ходе пленарного заседания и дискуссии за круглым столом подтвердили не только актуальность проблемы обеспечения информационной безопасности автоматизированных систем управления (АСУ) технологическими процессами (ТП) критически важных объектов (КВО), но и сложность задач, которые предстоит решать специалистам, чтобы обеспечить комплексную защиту производственных комплексов и отдельных объектов.

Открыл конференцию ведущий пленарного заседания **главный специалист по информационной безопасности ИПИ РАН Виктор Гаврилов**. Приветствие, направленное в адрес участников конференции **генеральным секретарем ОДКБ Николаем Бордюжей**, зачитал представитель ОДКБ Владислав Шушин. В тексте приветствия отмечена важность механизмов сотрудничества и развития международных отношений в области ИБ, в частности в сегменте противодействия преступлениям, совершаемым с применением информационных технологий. Как показывает практика, количество подобных преступлений за последние три года

возросло в сотни раз, стремительно увеличивается количество атак на объекты критически важной инфраструктуры. В настоящее время особенно актуальным является обсуждение концептуальных вопросов формирования международных и национальных систем защиты таких объектов, принципов кооперации и разделения компетенций, создания механизмов эффективного сотрудничества.

## Нормотворчество и безопасность КВО

Большое внимание на конференции было уделено тематике нормативно-правового



**Виктор ГАВРИЛОВ,**  
ИПИ РАН



регулирования в области безопасности критически важных объектов, в частности АСУ ТП. О состоянии работы над законопроектом об обеспечении безопасности критической информационной инфраструктуры Российской Федерации, концептуальных подходах к регулированию данной области рассказал **заместитель начальника департамента регулирования радиочастот и сетей Минкомсвязи России Георгий Грицай**. Среди основных принципов регулирования он назвал баланс интересов и взаимную



**Виталий ЛЮТИКОВ,**  
ФСТЭК России

ответственность личности, общества и государства в сфере обеспечения безопасности критической информационной инфраструктуры. При этом он предложил дополнить перечень таким принципом, как ликвидация последствий инцидентов и возможность восстановления инфраструктуры.

Одним из достижений данной редакции законопроекта представитель министерства считает полномочия Правительства восстанавливать порядок применения ресурсов сети связи общего пользования для обеспечения связью инфраструктурных объектов. Это даст возможность установить режим взаимодействия объектов критической инфраструктуры и сетей связи общего пользования. Что касается понятий критической информационной инфраструктуры и ее субъектов, то предлагаемая в законопроекте трактовка не содержит квалифицирующих признаков инфраструктуры, поэтому формулировка определений требует уточнений.

Завершается подготовка проекта 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. Об этом было рассказано в ключевом докладе конференции Виталия Лютикова, начальника управления ФСТЭК России. Он также сообщил об активной работе над документом представителей экспертного сообщества. На основе анализа российской и зарубежной нормативно-правовой базы и методических рекомендаций предлагается ряд мер по защите информации в АСУ ТП.

Рассказывая об основных положениях и структуре документа, представитель ФСТЭК России подробно остановился на его особенностях. Так, требования не распространяются на защиту



**Георгий ГРИЦАЙ,**  
департамент регулирования радиочастот и сетей Минкомсвязи России

секретной информации, предусматривают возможность применения средств защиты, прошедших оценку соответствия в любой из форм в соответствии с Законом № 184-ФЗ. Предлагается обеспечить согласованность мер по защите информации и мер по технологической безопасности, гибкий подход к выбору мер защиты информации в АСУ ТП, возможность принятия компенсирующих мер. Кроме того, предусмотрена альтернатива: оценка соответствия системы защиты АСУ ТП может быть выполнена в рамках приемочных испытаний системы либо аттестации. Виталий Лютиков разъяснил порядок выбора

мер по защите информации в рамках АСУ ТП. Взятый за основу базовый набор мер по защите информации, соответствующий установленному классу защищенности, адаптируется (применительно к структурно-функциональным характеристикам и особенностям АСУ ТП), уточняется (для адекватного блокирования или нейтрализации актуальных угроз) и дополняется (если необходимо) выполнить иные требования.

На вопросах комплексного подхода к разработке нормативной базы, методических рекомендаций, обеспечения связанности требований регуляторов, выполнимости устанавливаемых правил в сфере ИБ заострил внимание **Иван Мелехин, директор департамента консалтинга и аудита компании «Информзащита»**. Со ссылкой на конкретные законодательные акты он проанализировал, насколько выполнимы требования в их совокупности, указав на несогласованность трактовок и определений. Тем не менее до выхода новых нормативных правовых актов по защите КВО в рамках соответствующих работ можно обеспечить сбор информации о критичных объектах и результатах их категоризации по всем блокам, а также комплексные аудиты приоритетных типовых объектов. После издания правовых актов можно будет



**Иван МЕЛЕХИН,**  
компания «Информзащита»



**Руслан СТЕФАНОВ,**  
компания «ЭЛВИС-ПЛЮС»



**Вадим РЕЗОВ,**  
РФЯЦ-ВНИИЭФ



**Сергей ГАРБУК,**  
«Фонд перспективных исследований»



**Равиль САФИУЛЛИН,**  
ИВМ Россия и СНГ

определить целевые показатели защищенности АСУ ТП применительно к разным уровням их зрелости, разработать стандарты информационной безопасности систем. В стандартах следует закрепить требования по ИБ к поставщикам АСУ ТП. Наряду с этим важно сформировать программу контроля защищенности систем управления (регулярные проверки, отчетность, информирование об инцидентах) и программу аудитов на соответствие разработанным стандартам. Предстоит также создавать тестовые среды по анализу компонентов АСУ ТП.

Тема классификации АСУ ТП и оценки защищенности систем на примере опыта системного интегратора применительно к проблеме разработки и совершенствования нормативно-правовой базы стала центральной в выступлении **Руслана Стефанова, ведущего инженера Центра комплексных услуг и проектов компании «ЭЛВИС-ПЛЮС»**. Главная задача защиты АСУ ТП КВО – недопущение несанкционированного доступа к объектам управления (прямых команд управления, изменения параметров режима и противоаварийной защиты, а также подмены значений измерений).

Для анализа критериев классификации следует учитывать категорию опасности объекта, степень связанности системы (информации) и возможного ущерба (значимость, характер влияния и масштаб самой системы). Оптимальную классификацию сложных систем можно обеспечить путем определения зависимости классифицируемой системы и взаимодействующих с ней систем. В рамках аудита систем как одного из этапов реализации проектов специалисты компании «ЭЛВИС-ПЛЮС» ищут ответы на вопросы, каким угрозам подвержена и насколько защищена система, какие мероприятия необходимо выполнить для повышения уровня ее защищенности. Методика аудита предусматривает проведение аналитического и практического исследований. После того как определены приоритетные направления защиты, составляется план мероприятий по нейтрализации актуальных угроз и определяется стоимость работ.

## Трансформация угроз как тренд на перспективу

Обзор ключевых направлений разработки технологий, позволяющих парировать перспективные угрозы ИБ критически важных инфраструктур, представил **Сергей Гарбук, заместитель генерального директора «Фонда перспективных исследований»**. Созданный полтора года назад фонд содействует осуществлению научных исследований и разработок в интересах обороны страны и безопасности государства. По мере развития АСУ ТП угрозы информационной безопасности трансформируются. К числу перспективных задач обеспечения ИБ представитель



Стенд компании «Информзащита»



Стенд компании «ЭЛВИС ПЛЮС»



Стенд компании «АМТ-ГРУПП»



Стенд ООО «Газинформсервис»



Стенд ООО «УЦСБ»



Стенд компании IBM

фонда от-  
нес разработку  
технологий автоматической  
проверки исполняемого кода  
на отсутствие недекларированных  
возможностей, создание средств  
защиты информации в недоверен-  
ной среде, каналов управления  
и телеметрирования систем (на  
основе технологий квантовой крипто-  
графии), а также распределенных  
систем мониторинга состояния  
объектов КВО в целях  
построения интеллек-  
туальных поведенче-  
ских моделей, учиты-  
вающих ценностные  
и смысловые аспекты  
реализуемых тех-  
нологических  
процессов.

Система  
информационной  
безопасности не может  
служить дополнением к готовой  
системе автоматизации. А ведь  
такой подход зачастую предпо-  
читают специалисты в сфере  
проектирования, управления пред-  
приятием, сетевых технологий,  
которые действуют исходя из луч-  
ших практик, оставляя решение  
вопросов ИБ на «потом». Как по-  
казывает опыт внедрения типовых  
информационных систем на пред-  
приятиях ядерно-оружейного ком-  
плекса, основу успешного созда-  
ния АСУ ТП КВО составляет сис-  
темное проектирование. К такому  
выводу пришел в высту-  
плении на конферен-  
ции **представитель**

### РФЯЦ-ВНИИЭФ Вадим Резвов.

По его мнению, эффек-  
тивность информационной  
безопасности закладывается на  
этапе проектирования комплекс-  
ного защищенного технического  
решения, которое должно обес-  
печивать взаимодействие систем  
управления предприятием, про-  
изводством, технологическими  
процессами и систем 3D-проекти-  
рования. В настоящее время раз-  
работан проект стандарта Госкор-  
порации



Росатом «Порядок создания автоматизированных систем в защищенном исполнении».

О комплексном предложении IBM для контроля активности в масштабе предприятия на пленарном заседании конференции рассказал **Равиль Сафиуллин, руководитель направления по работе с ключевыми заказчиками, IBM Россия и СНГ**. При разработке решения полного цикла специалисты корпорации учитывали, в частности, такие вызовы ИБ, как обнаружение угроз, в том числе со стороны инсайдеров, консолидация массивов данных, прогнозирование рисков для бизнеса, соблюдение требований регуляторов. Основными «козырями» решения полного цикла IBM являются интеллект (проактивное управление угрозами, быстрый анализ способов воздействия), интеграция (поддержка Big Data, аппаратная платформа и экспертиза) и автоматизация (быстрое внедрение, экосистема решений с открытым кодом, операционная эффективность).

Детально с решениями IBM в сфере информационной безопасности, разработанными, в частности, для электроэнергетических компаний, участники конференции смогли ознакомиться в ходе технического семинара IBM, состоявшегося в рамках мероприятия. **Роман Андреев,**

**технический специалист IBM,** представил продукт QRADAR Security Intelligence, предназначенный для обнаружения инцидентов ИБ в корпоративной сети, выявления инсайдерских угроз, рисков неправильной конфигурации сетевого оборудования, а также контроля над соблюдением нормативных требований и стандартов.

Особенностям построения высокопроизводительных, отказоустойчивых и защищенных от несанкционированного использования геоинформационных систем двойного назначения на основе контекстно-зависимых вычислительных технологий посвятил свое выступление **Андрей Чепелев, заместитель директора ФГУП ЦНИИ «Центр»**. С докладчиком **профессор Геннадий Алакоз** представил программно-техническое решение отечественного производства для построения систем защиты критически важных объектов. Научная база для этой разработки была заложена еще в советское время.

О проблемах в сфере комплексной информационной безопасности промышленных объектов (от периметра до исполнительных устройств) и вариантах их решения рассказал **Алексей Мальнев, начальник отдела защиты КСИИ «АМТ-ГРУП»**. Комплексный подход

к безопасности обеспечивается на всех уровнях, для всех векторов атак, а степень ИБ определяется слабейшим звеном в системе. При реализации специализированного подхода в расчет принимаются только необходимые и допустимые для АСУ ТП средства информационной безопасности, учитывается контрольно-измерительная информация. В настоящее время уровень реальных ИБ-угроз достиг такой отметки, что приходится анализировать многочисленные риски, поскольку, как показывает практика, незначительных угроз не бывает. Важнейшая составляющая ИБ АСУ ТП – периметр. Но его задача – свести к минимуму внешние угрозы, поэтому концентрироваться только на периметре опасно. Компания АМТ-ГРУП предлагает решение, позволяющее устранить большую часть внешних угроз. Проектирование сетевого дизайна локальных вычислительных сетей АСУ ТП, который напрямую влияет на защищенность и устойчивость системы в целом, в большинстве случаев неразрывно связано с проектами ИБ.

Анализируя частные вопросы защиты информации в АСУ ТП КВО, **Павел Алексеев, начальник отдела ОАО «Газинформсервис»**, заострил внимание на необходимости контролировать изменения конфигурации таких систем и используемых в них средств защиты, рассказал о конкретном решении, которое может применяться для этих задач.

**Алексей Полянский, генеральный директор научно-технического центра «Станкоинформзащита»**, на конкретных примерах из практики проанализировал риски при обслуживании и выполнении гарантийных обязательств поставщиком станков с ЧПУ иностранного производства. Особое внимание он уделил способам минимизации подобных рисков с помощью систем обнаружения вторжений, программных и технических средств защиты, построенных с учетом специфики оборудования с ЧПУ.



Технический семинар компании IBM

## Энергетический контур ИБ

Одним из самых обстоятельных и интересных, по отзывам делегатов конференции, стало выступление **Андрея Корнеева, руководителя Центра проблем энергетической безопасности Института США и Канады РАН**. В докладе, посвященном рефлексивному управлению обеспечением безопасности АСУ ТП, он заострил внимание на трудностях перехода к интеллектуальным энергетическим сетям, проанализировал преимущества методики сценарного моделирования, на основе которой можно обеспечить информационно-психологическую безопасность с учетом проблемы человеческого фактора. Одновариантные прогнозы в сфере безопасности, задающие единственную линию будущего развития, часто оказываются ошибочными. При сценарном подходе разрабатывается несколько наиболее вероятных, но контрастных вариантов будущего развития враждебной внешней среды. Стратегическое планирование энергетической безопасности означает рефлексивное системное управление на основе инвариантного предвидения вероятностных изменений.

В рамках сценарного прогнозного моделирования с обратной связью определяются ключевые стратегические альтернативы действий, устанавливаются опасные факторы внешней среды, угрозы ранжируются по важности и степени неопределенности, выявляется альтернативная логика развития каждого сценария, обеспечивается модификация перспективного плана действий, оценивается устойчивость возможных стратегических решений, разрабатываются индикаторы эффективной системы раннего обнаружения возможных угроз безопасности.

Методику сценарного моделирования Андрей Корнеев представил в виде семи последовательных шагов: определить стратегические направления; установить ключевые факторы внутренней и внешней среды; ранжировать



Роман АНДРЕЕВ представляет продукт компании IBM QRADAR Security Intelligence

по важности и степени неопределенности; выявить логику динамики каждого сценария; обеспечить «очистку» инвариантных сценариев по критериям важности; сформулировать выводы и тактические рекомендации; определить характерные индикаторы контроля управления.

В современных условиях рост уязвимости новых автоматизированных производственных систем сопровождается опасной критичностью самого слабого звена бизнес-управления – человеческого фактора. Как известно, правильно обучать и заранее тренировать людей обходится намного дешевле, чем ликвидировать последствия аварий. Комплекс средств обеспечения безопасного функционирования современных автоматизированных энергетических систем должен включать следующие блоки обязательной защиты: от общей некомпетентности и безответственности персонала, нарушений целостности и режимов работы сетевых коммуникаций, вскрытия и злонамеренной переналадки аппаратуры, сознательного коррупционного небрежения в отношении мер безопасности, враждебных и предательских инсайдеров, военного и промышленного шпионажа.

Для снижения рисков, связанных с человеческим фактором, методика первичного обучения

и непрерывного повышения квалификации персонала должна включать не менее пяти обязательных этапов: мультимедийный рассказ преподавателя с использованием программированных учебных пособий, на основе конкретных критических ситуаций и примеров; показ преподавателем на диспетчерских тренажерах практических примеров действий по ликвидации аварийных ситуаций; совместная командная работа преподавателей и обучаемых на тренажерах и прохождения контрольных тестов в условиях повышенной неопределенности; самостоятельная индивидуальная и групповая работа обучаемых по практическому применению полученных навыков под наблюдением преподавателей; зачетное индивидуальное прохождение обучаемыми производственных стресс-тестов с моделированием критических ситуаций и последующей защитой квалификационной работы с анализом ошибок и корректирующими рекомендациями.

Вопросы обеспечения энергетической безопасности выбрал в качестве темы выступления на конференции **Георгий Петросюк, начальник отдела информационной безопасности Управления корпоративной защиты «Мосэнерго»**. Среди множества проблем, возникающих при проектировании АСУ ТП, он выделил



**Георгий ПЕТРОСЮК,**  
Мосэнерго

нехватку специалистов по ИБ и недостаточную компетенцию проектировщиков в этой области, отсутствие у проектировщиков мотивации к созданию защищенных с точки зрения информационной безопасности систем АСУ ТП, а также специализированных средств ИБ. Реализация устаревших архитектурных и аппаратных решений при проектировании, применение недоверенных аппаратных и программных средств наряду с использованием компонентов иностранного производства или привлечением иностранных разработчиков создают дополнительные препятствия в сфере проектирования АСУ ТП.

По словам **Олега Маслова, начальника службы информационной безопасности Управления безопасности компании «Тюменьэнерго»**, автоматизированные системы управления технологическими процессами – неотъемлемая часть современного электросетевого комплекса. Любое изменение целостности или доступности информации, обрабатываемой в АСУ ТП, может привести к нарушению технологического процесса, а значит, спровоцировать возникновение чрезвычайной ситуации, финансовые потери и другие негативные события. Безопасность АСУ ТП существующих объектов обеспечивается на трех уровнях: применение стандартных

мер и средств защиты; развертывание специализированных средств и построение доверенной среды функционирования АСУ ТП. В условиях создания «умных сетей» актуальность вопросов информационной безопасности выходит на первый план.

## Интеграция технологий и решений

Опыт и решения Уральского центра систем безопасности представил **Николай Домуховский, главный инженер департамента системной интеграции**



**Олег МАСЛОВ,**  
компания «Тюменьэнерго»

**ООО «УЦСБ»**, который рассказал о приоритетных направлениях и мерах защиты элементов АСУ ПТК (превентивных, детективных и корректирующих). Среди актуальных задач обеспечения безопасности АСУ ПТК докладчик назвал развитие взаимодействия отраслевых регуляторов и владельцев, производителей (разработчиков) систем, разработку единых подходов к защите АСУ ПТК (типовые архитектуры систем защиты для элементов систем, встраивание механизмов защиты на этапе разработки, оптимизация решений по автоматизации ТП). Николай Домуховский предложил

сформировать общий репозиторий инцидентов АСУ ПТК (в масштабе предприятия и отрасли). Повышению уровня доверия к элементам таких систем будут способствовать оценка соответствия элементов АСУ ПТК требованиям по ИБ (отраслевая, национальная), а также проактивный поиск уязвимостей.

Аргументы в пользу применения технологии совместной обработки и хранения информации различных уровней конфиденциальности в АСУ ТП на предприятиях оборонно-промышленного комплекса представил **Владимир Гордейчук, исполнительный директор Закрытого научно-производственного акционерного общества «Отделение проблем военной экономики и финансов»**. Но реализация этого подхода требует проработки вопросов в части совершенствования нормативно-методической базы, создания и использования специализированной технологической системы, обеспечивающей гарантированный уровень безопасности при обработке и хранении информационных ресурсов АСУ ТП.

На экономическую составляющую вопросов безопасности обратил внимание участников конференции **Павел Овчинников, заместитель заведующего кафедрой факультета инноваций и высоких технологий МФТИ,**



**Николай ДОМУХОВСКИЙ,**  
ООО «УЦСБ»

в докладе «Создание защищенных автоматизированных систем с использованием программных решений на платформе «1С:Предприятие». Представляя интеграционную технологическую платформу «1С:Интеграция», выступающий отметил, что основное назначение программно-методического комплекса – повышение эффективности управления группой компаний за счет управления информационными потоками из единого центра (передача данных, контроль доставки и обработки данных), обеспечения информационных связей между разрозненными информационными системами и управления распределенными приложениями в реальном времени. Наибольший эффект от внедрения достигается при совместном использовании с шиной передачи данных (разработка «1С» – МФТИ) и набором специализированных адаптеров.

## Практика защиты

Второй день работы конференции открылся серией докладов, посвященных практическим подходам к созданию защищенных АСУ ТП.

О том, как можно тестировать защищенность АСУ ТП и отдельных ее компонентов на макетах, рассказал **директор**

**департамента АСУ НТЦ «Станкоинформзащита» Александр Бурцев.** Преимущество макета – возможность внесения изменений в систему, чего нельзя делать на реальных объектах. В макетах используются те же компоненты, что и в системах управления на действующих объектах, – специализированные устройства, специализированное ПО, алгоритмы управления, иногда воспроизводятся технологические процессы разной степени детализации. Набор компонентов зависит от назначения испытательного стенда. На макетах могут проверяться: уязвимости оборудования и ПО отдельных узлов и элементов системы; надежность и эффективность, а также совместимость СЗИ; возможные векторы атак на отдельные элементы системы; устойчивость применяемых алгоритмов управления к внешним воздействиям. При необходимости могут оцениваться последствия вредоносных воздействий (в том числе финансовые риски), однако построение макетов столь высокой степени детализации зачастую экономически нецелесообразно.

**Заместитель директора по развитию ООО «Системы информационной безопасности» (СИБ) Руслан Пермяков** напомнил, что особенности АСУ ТП (в отличие от офисных АСУ) – работа в реальном времени,

высокая сложность, ограниченные возможности использования активных методов защиты, отсутствие в АСУ ТП конфиденциальной информации.

Основной вопрос при работе с АСУ ТП – доверие: к источнику, к каналу, к получателю информации (терминалу). Причем уровень доверия может изменяться. В современных АСУ ТП проблема доверия во многом обусловлена широким применением автоматизированных решений. АСУ ТП взаимодействуют со средами другого назначения (офисной сетью, Интернетом), а авторизация устройств и принятие решений могут осуществляться без участия человека. По сути, возникает задача стыковки различных систем, при этом необходимо обеспечить процедуры контроля их изменений во времени. Специалисты СИБ пришли к выводу о необходимости обособления сторон информационного обмена и организации проверки отправляемой информации, среды передачи, верификации санкционированных изменений в системе. На сегодня предлагаются решения, работающие на верхнем уровне АСУ ТП, – применение криптографических протоколов, проверка ограниченных условий, проверка на соответствие моделям. Используются аккумуляция данных и корреляционный анализ, а также процедуры независимой проверки поступающей информации. В развитие подхода в компании разрабатывается программно-аппаратное решение для сбора и оперативного анализа информации о состоянии системы – пассивная система, которая не вмешивается в работу объекта защиты.

**Руководитель Инжинирингового центра Национального исследовательского ядерного университета МИФИ Дмитрий Михайлов** акцентировал внимание на проблемах защиты АСУ ТП на нижнем уровне (уровне полевых устройств). Как правило, верхний уровень АСУ ТП (уровень диспетчерского управления) является только входом в систему, а атаки злоумышленников направлены на



**Александр БУРЦЕВ,**  
АСУ НТЦ «Станкоинформзащита»



**Руслан ПЕРМЯКОВ,**  
ООО «Системы информационной безопасности» (СИБ)



нижележащие уровни (кстати, выкладывая в Интернет фото своих рабочих мест с отраженной на мониторе архитектурой АСУ ТП или организовав удаленный SSH-доступ к системе SCADA, беспечные сотрудники помогают злоумышленникам найти вход).

Чтобы добраться до уровня ПЛК, хакерам потребуется больше знаний плюс определенные организационные мероприятия. Ошибки компаний, действующие на руку хакерам, – переоценка принятых мер физической безопасности (контроля доступа к техническим помещениям), а также публикация подробных описаний выполненных проектов, которые могут помочь злоумышленнику восстановить архитектуру АСУ ТП.

Но меньше всего развиты средства защиты на полевого уровне. Например, редко бывают защищены передающие линии на объектах. Решение, предлагаемое Инжиниринговым центром, – устройство низового уровня, которое определяет наличие несанкционированного подключения к датчикам и линиям передачи данных системы управления. Докладчик отметил, что моделирование, о котором говорилось в прозвучавшем ранее докладе, важно для отработки подобных решений.

**Антон Волков, старший преподаватель кафедры безопасности информационных систем ГОУ ВПО «Самарский государственный университет»,** рассмотрел структуру процесса защиты АСУ и рассказал об особенностях построения алгоритма автоматизированного построения комплексной системы защиты информации. В целом процесс защиты информационной системы состоит из двух этапов: аудит и формирование требований к защите на основании законодательства, отраслевых требований и модели угроз; построение системы защиты. В общем виде алгоритм построения комплексной системы защиты информации следующий: 1) выбор основных элементов системы (для начала можно взять уже имеющиеся средства и дополнить их необходимыми,

чтобы закрыть требования законодательства); 2) выбор дополнительных элементов – доработка системы защиты информации, чтобы она стала комплексной; 3) анализ и оценка созданной системы защиты информации – проверка на отсутствие противоречий между выбранными средствами, на степень пересечения функционала, 4) коррекция и перезапуск алгоритма, если система не полностью удовлетворяет выработанным критериям. Следует отметить, что к числу средств защиты информации относятся программные, программно-аппаратные, инженерно-технические комплексы, а также организационные меры. Описать их математически не всегда просто, особенно последние. Еще одна сложность для математического описания – учет внешних факторов, влияющих на алгоритмы построения системы защиты (принятых в отрасли практик, предпочтений руководства, компетенций специалистов, условий лицензирования продуктов и др.). Специалисты кафедры предлагают для этого свои ноу-хау.

## Наука и жизнь

**Эдик Аракелян, профессор кафедры АСУ ТП НИУ «МЭИ»,** остановился на особенностях

АСУ ТП современных тепловых электростанций. Сегодня на одной станции может присутствовать несколько типов АСУ ТП и в составе каждой из них – несколько программно-технических комплексов (ПТК) разных производителей. Технически и технологически российская энергетика находится в большой зависимости от зарубежных стран. Современные АСУ ТП электростанций образуют распределенную иерархическую сеть, и распределенность создает благоприятные условия для атак на низовую автоматику. С учетом этого концепция защиты объектов энергетики должна предусматривать создание безопасных автоматизированных систем, работающих в недоверенной среде.

Среди выявленных в отрасли проблем – низкий уровень информационной безопасности на всех иерархических уровнях управления вследствие недопонимания заказчиками значимости ИБ и желания снизить стоимость ПТК. Кроме того, нет четких методик учета требований ИБ на этапе проектирования АСУ ТП.

По мнению докладчика, необходимо описание типовых сценариев скрытого управления АСУ ТП. Для защиты нужны проактивные и активные методы. Активная защита предполагает создание механизмов доверия к элементам



АСУ ТП, а это потребует проектирования систем безопасности одновременно с технологическими процессами. Перспективной представляется концепция защиты АСУ ТП на основе поведенческой модели. Важный вопрос – проработка законодательной базы в области защиты критически важных объектов. Проблемой является также отсутствие специалистов по ИБ, понимающих специфику АСУ ТП.

В России нет стандартов в области обеспечения безопасности АСУ ТП, констатировал **консультант по разработке стандартов для АСУ ТП, выпускник программы РАНХиГС по специальности MBA Chief Security Officer Александр Баскаков**. В мире популярен американский стандарт NIST, есть и другие стандарты (NERC CIP, 20 Critical Security Controls и пр.), но они больше ориентированы на технические меры и не учитывают необходимости подходить к обеспечению безопасности как к процессу управления. Для организации процесса управления требуется прежде всего определить уровень развития управляемой структуры. Делается это на основе так называемой модели зрелости. Автор проанализировал существующие в мире модели зрелости и предложил собственную модель зрелости процесса обеспечения безопасности бизнеса. Модель содержит ряд метрик, позволяющих определить существующий уровень реализации мер безопасности на предприятии, обеспеченность процесса управления безопасностью необходимыми ресурсами, уровень ответственности участников процесса, степень участия руководства и др. В структуру проекта стандарта безопасности АСУ ТП наряду с традиционными существующими разделами «Общая характеристика объекта защиты» и «Описание требований к мероприятиям защиты» предлагается внести блок, посвященный управлению процессом безопасности на уровне АСУ ТП. В него должны входить модель зрелости и функциональная



модель процесса обеспечения безопасности, содержащая описание подпроцессов процесса управления безопасностью АСУ ТП.

Чтобы эффективно управлять, нужно уметь качественно прогнозировать риски и обосновывать меры защиты в режиме упреждения, убежден **Андрей Костокрызов, главный научный сотрудник, профессор ИПИ РАН и председатель подкомитета информационной и промышленной безопасности Комитета по безопасности предпринимательской деятельности Торгово-промышленной палаты РФ**. В существующих стандартах управления безопасностью в различных средах содержится требование управления рисками. Но риск каждый понимает по-своему. Профессор Костокрызов с коллегами проанализировали существующую нормативно-методическую базу в различных областях. В большинстве областей нет вероятностной оценки рисков, задаются лишь требования выполнения тех или иных условий/действий для обеспечения безопасности. Во всех документах приветствуются ситуационный анализ потенциально опасных событий, мониторинг состояний и меры оперативного восстановления, хотя на деле это обеспечивается далеко не всегда. Применяемые методы анализа

рисков тоже различаются. Многие методы основаны на экспертных оценках (т. е. субъективны), они не позволяют обосновывать понятие допустимых рисков. Нет моделей для анализа рисков, обеспечивающих возможность решать обратные задачи обоснования требований к системам сбора и анализа информации, параметрам контроля и мониторинга.

Решить проблемы прогнозирования рисков, а главное, обосновать понятие допустимого риска и применение превентивных мер позволяют вероятностные модели. Идея в том, чтобы количественно оценивать степень рисков на протяжении всего жизненного цикла системы и задавать упреждающие требования.

Вопросам повышения квалификации специалистов, занимающихся защитой информации в ключевых системах информационной инфраструктуры, посвятил свой доклад **заведующий кафедрой «Информационная безопасность» НОУ ДПО «Северо-западный центр комплексной защиты информации» (СЗЦКЗИ) Владимир Киреев**. Центр проводит дополнительное профессиональное обучение по девяти программам, в том числе «Организация мероприятий по обеспечению безопасности информации в КСИИ». Одна из проблем в этой области заключается в том,



что руководители не понимают, что именно они должны защищать, что на их объектах относится к гостайне, а что к ключевым информационным системам. Это не удивительно, если учесть, что сегодня законодательно определены 17 видов тайн, 25 видов конфиденциальной информации, 10 видов информации ограниченного доступа.

По мнению докладчика, следует отказаться от многочисленных систем классификации информационных систем, создав единую, понятную и несекретную. Необходимо определить минимально необходимый и достаточный комплект законодательных и нормативных документов, а также типовой состав организационно-распорядительных документов организации и обеспечить этими документами подразделения по защите информации. Типовой состав таких подразделений на предприятиях должны определить регуляторы. Кроме того, следует определить и узаконить временные затраты специалистов по защите информации на разработку организационно-распорядительных документов.

## Дискуссионные вопросы

По окончании пленарной сессии состоялся круглый стол.

На обсуждение были вынесены вопросы нормативного и методологического обеспечения защиты АСУ ТП критически важных объектов, специфики рисков и угроз АСУ ТП КВО; проблематика применяемых организационных мер и технических средств защиты информации, обрабатываемой в АСУ ТП; проблемы компетенции специалистов-практиков и вопросы ответственности за функциональную и информационную безопасность АСУ ТП. Заседание провел **главный специалист по информационной безопасности ИПИ РАН Виктор Гаврилов.**

Очевидно, что подлинная безопасность АСУ ТП может быть реализована только совместными усилиями специалистов по информационной безопасности и специалистов по промышленной (функциональной) безопасности. Традиционные регуляторы в области ИБ не занимаются вопросами функциональной безопасности в конкретных отраслях.

Функциональная безопасность включает среди прочего механизмы защиты от ошибок при проектировании систем и алгоритмов функционирования объекта.

С этой точки зрения заслуживает внимания опыт концерна «Росэнергоатом», о котором рассказал **Александр Комов, главный эксперт департамента**

**информационных технологий «Росэнергоатома».** Обязательными документами для «Росэнергоатома» являются федеральные нормы и правила (ФНП) в области использования атомной энергии. Проверять их выполнение уполномочен «Ростехнадзор». Подтверждение выполнения ФНП «Ростехнадзор» осуществляет путем выдачи лицензий проектировщикам, конструкторам, монтажникам и эксплуатационникам. Таким образом, система ФНП обеспечивает равную надежность системы во всей цепочке работ от проектирования до технического обслуживания.

Проектант обязан составить список проектных аварий, для каждой из них проектируется система безопасности, которая должна предотвратить проектную аварию. В проекте содержится техническое обоснование безопасности, где вероятностными методами доказывается, что вероятность тяжелых аварий составляет меньше  $10^{-7}$ , и детерминистическими методами – необходимость соблюдения установленных требований. Класс безопасности создаваемой системы устанавливает проектант.

Конструктор должен спроектировать систему безопасности, которая удовлетворяет



обязательные требования. В обязательных требованиях записано, в частности, что система безопасности должна выполнять свои функции при любом отказе и (что важно) любой ошибке персонала. Каждый элемент системы должен непрерывно диагностироваться, в противном случае он считается отказавшим.

Как отметил спикер, выполняя обязательные требования промышленной безопасности, конструктор тем самым выполняет и требования информационной безопасности. Тем более что для атомной энергетики требования промышленной безопасности (в данном случае ядерной и радиационной) сейчас более важны, чем требования защиты от злоумышленников. Системы безопасности «Росэнергоатома» не связаны с внешним миром, имеют собственную систему электропитания. В ее основе лежит полностью переработанная зарубежная разработка, для нее создана собственная элементная база.

Однако не во всех отраслях предприятия чувствуют себя столь уверенно. Компании работают в коммерческой среде и зачастую при выборе АСУ ТП руководствуются исключительно экономическими соображениями. Между



тем на рынке присутствуют самые разные разработки, в том числе выполненные на открытой элементной базе, а ПО для SCADA может быть даже «самописным». Поэтому хорошо было бы иметь официальный список рекомендуемых систем. Для энергетической отрасли, например, есть списки систем, аттестованных Минэнерго, действует сертификационный центр НТЦ ФСК ЕЭС, однако никто никогда не проводил проверки SCADA на скрытые коды.

Участниками обсуждения высказывались также сомнения в целесообразности предоставления собственнику права самостоятельно определять класс АСУ и требования к оборудованию, в частности потому, что без давления со стороны государства собственник будет принимать только те решения, которые ему экономически выгодны.

По поводу финансового аспекта **Виктор Гаврилов** отметил следующее: согласно проекту закона «О безопасности критической информационной инфраструктуры Российской Федерации» финансирование мероприятий по обеспечению безопасности КИИ осуществляется владельцем объекта, а также за счет средств федерального бюджета, выделенных уполномоченным федеральным органам исполнительной власти.

Что касается «давления со стороны регулятора», то будущий документ ФСТЭК «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах...», по сути, является обязательным. Предполагается, что собственник достаточно хорошо знает свой объект, чтобы выявить актуальные угрозы и определить класс АСУ, после чего он выполняет требования безопасности для соответствующего класса систем.

В части организационных и методических аспектов подготовки проекта создания АСУ ТП опытом поделился **Николай Домуховский (ООО «УЦСБ»)**. С точки зрения основных этапов такой проект ничем не отличается от создания любой другой АСУ в защищенном исполнении. За основу можно брать ГОСТ Р 51583. Определенные отличия могут иметь отдельные стадии проекта, например моделирование угроз. Здесь можно воспользоваться зарубежным опытом – научными работами, методиками. Одна из таких методик – доработанный вариант анализа живучести автоматизированной системы (моделирование отказов) – применима для построения моделей угроз АСУ ТП. Что касается средств защиты АСУ ТП, то



это должны быть специализированные средства, которые прошли предварительное тестирование на стендах. Одна из сложностей подобного проекта в том, что специалисты по ИБ не понимают специфики работы АСУ ТП и им необходимо специально погружаться в тему.

В процессе обсуждения технических средств защиты АСУ ТП была поднята проблема защиты давно созданных систем, работающих на операционных системах и аппаратных компонентах, которые уже не поддерживаются производителями. В этих условиях защита старых АСУ ТП оказывается проблемой более сложной, чем проектирование новых. Частичным решением проблемы зависимости от аппаратного АРМ могло бы стать использование терминального доступа, но практика поддержки терминальных решений среди производителей АСУ ТП не распространена.

Кроме того, производители защитного ПО (антивирусов) не поддерживают работу своих продуктов со старыми ОС. С другой стороны,

производители АСУ ТП и технических средств охраны, даже если и соглашаются на установку стороннего антивируса на свою систему, задают для него жесткие ограничения, поскольку стандартные антивирусные пакеты не всегда «дружат» с системами АСУ ТП и ТСО.

Отсюда предложение: функция выбора средств защиты для ТСО и АСУ ТП должна принадлежать проектировщику или сопровождающей организации, а не собственнику системы. Возможно, было бы целесообразно ввести сертификацию СЗИ на уровне производителя, чтобы тот мог сам предлагать адекватные средства защиты.

Между тем вопрос о сертификации СЗИ конкретного производителя достаточно сложен, поскольку ведущие производители АСУ ТП проявляют закрытость в части своих систем. Как считает **Руслан Пермяков (ООО «СИБ»)**, некоторые задачи ИБ можно переложить со средств, устанавливаемых непосредственно на защищаемые объекты, на устройства защиты, которые устанавливаются рядом с объектами. Такое

устройство не будет отнимать ресурс у защищаемого процесса, кроме того, его можно конфигурировать в широких пределах.

Последним пунктом обсуждения стал вопрос о профессиональных компетенциях специалистов, занимающихся защитой АСУ ТП. Как считает **Руслан Стефанов («ЭЛВИС ПЛЮС»)**, ближе всего к цели защиты АСУ ТП стоят системные интеграторы, которые занимаются созданием АСУ ТП, — они лучше знают систему и могут кооперироваться с компаниями, работающими в сфере ИБ, или создавать собственное подразделение, специализирующееся на ИБ.

Что же касается подготовки специалистов, то, как отметил профессор **Эдик Аракелян (МЭИ)**, необходимо сочетание двух специальностей — по эксплуатации АСУ ТП и по информационной безопасности. Но для подготовки таких специалистов нужна соответствующая научно-производственная база, включая специализированные стенды. Требуются также совместные усилия всех заинтересованных участников рынка. ■



# Рекомендации конференции «Информационная безопасность АСУ ТП КВО»

По результатам обсуждения широкого круга тем, связанных с обеспечением информационной безопасности критически важных объектов, – от вопросов нормативного регулирования до практики защиты ИБ АСУ ТП КВО, а также по итогам дискуссии на состоявшемся в рамках конференции круглом столе участники конференции считают нужным выдвинуть ряд инициатив, которые будут способствовать постепенному решению существующих в данной области проблем.

1. В целях обеспечения единства подходов и гармонизации терминологии в области обеспечения безопасности АСУ ТП участники конференции рекомендуют обратиться в Федеральное агентство по техническому регулированию и метрологии (Росстандарт) с предложением включить в программу разработки национальных стандартов Российской Федерации на 2015 год работу по подготовке национального стандарта «Безопасность автоматизированных систем управления производственными и технологическими процессами».

2. Рекомендовать отраслевым регуляторам (профильным министерствам) выработать правовые механизмы, позволяющие привлекать к выполнению работ по обеспечению безопасности АСУ ТП КВО организации, имеющие не только аккредитацию в установленном порядке, но и опыт автоматизации управления и решения задач функциональной безопасности АСУ ТП в соответствующей отрасли.

3. В целях повышения эффективности защиты информации в АСУ ТП участники конференции считают нужным обратить



внимание компаний, специализирующихся в области разработки средств защиты информации, на необходимость создания специализированных средств защиты АСУ ТП, учитывающих специфику их эксплуатации, в том числе работу в режиме реального времени и длительность жизненного цикла. Создание новых и модернизация существующих средств защиты АСУ ТП должны производиться с учетом требований федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, а также с учетом требований функциональной безопасности АСУ ТП со стороны отраслевых регуляторов.

4. Участники конференции считают необходимым отметить, что эффективное решение проблемы

безопасности критически важных объектов информационной инфраструктуры Российской Федерации невозможно без разработки и организации производства отечественной электронной элементной базы и программного обеспечения.

5. Участники конференции считают целесообразным обратиться в Минобрнауки с предложением наладить подготовку кадров, компетентных в сфере защиты АСУ ТП. С этой целью учебным заведениям, осуществляющим подготовку специалистов по информационной безопасности и подготовку специалистов в области функциональной безопасности объектов, при составлении учебных планов учитывать специфику обеспечения информационной безопасности АСУ ТП. Рассмотреть возможность подготовки отдельной категории специалистов – в области информационной безопасности АСУ ТП. ■