Концепция обеспечения защиты от несанкционированного доступа АСУТП АЭС "Бушер-1"

А.Г. Полетыкин, В.Г. Промыслов, Н.Э.Менгазетдинов (ИПУ РАН)

Предложен новый способ создания системы защиты от несанкционированного доступа в АСУТП, обеспечивающий комплексную защиту от преднамеренных и непреднамеренных вредных воздействий на элементы ПО со стороны различных групп пользователей.

Введение

Массированное внедрение программируемых средств в АСУТП АЭС породило новую проблему – как защитить ПО. Чаще всего эту проблему ассоциируют с "защитой от несанкционированного доступа" (ЗНСД) [1], то есть с деятельностью, определяемой как "предотвращение получения защищаемой информации заинтересованным субъектом с нарушением прав или правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации" [2]. Однако данный подход не отвечает всем требованиям по обеспечению безопасности эксплуатируемого объекта. Необходимо включить в определение действия по защите информации от непреднамеренного воздействия (ЗИНВ), призванную предотвратить негативное воздействие на защищаемую информацию от ошибочных операций пользователя, сбоя технических и программных средств информационных систем.

Необходимо констатировать, что для АСУТП АЭС санкционированный, но ошибочный доступ может представлять серьезную опасность, если в результате выполняемых действий нарушается целостность ПО АСУТП. Далее будем рассматривать ЗНСД как комплексную задачу защиты от непреднамеренного воздействия.

Актуальность ЗНСД в АСУТП почти ни у кого не вызывает сомнений, особенно в свете возросшей террористической угрозы и опасности техногенной катастрофы. Но в массовом сознании ЗНСД ассоциируется с защитой от вирусов, запретом игр на рабочем месте и прочими бедами бытовых и офисных компьютеров. Поэтому лица, принимающие решения, считают подчас, что проблема ЗНСД АСУТП АЭС аналогична проблеме защиты корпоративных офисных сетей. Однако это не так – перенесение методов ЗНСД с офисных сетей на АСУТП АЭС неправомерно и неправильно. Более того, как будет показано ниже, ряд методов, реализуемых при решении ЗНСД в общедоступных информационных системах просто нельзя применять в АСУТП.

Отличительной особенностью АСУТП АЭС от бытовых и корпоративных вычислительных сетей является то, что они представляют собой комплекс сильно связанных элементов, выполняющих единые функции по управлению объектом автоматизации [3, 4]. Другое характерное отличие АСУТП АЭС как сложной системы – это неполная определенность ее поведенческой модели, что затрудняет анализ безопасности системы. Рассмотрим проблемы обеспечения ЗНСД АСУТП АЭС с учетом вышеизложенных особенностей.

Обзор применяемых методов ЗНСД в АСУТП

Рассматривая классификацию систем ЗНСД можно выделить два класса:

- "глухая защита", т.е. защита, реализующая максимальный комплекс мер по предотвращению несанкционированного доступа (НСД), в том числе и меры по физическому ограничению доступа;
- защиты с использованием некоторой единичной организационно-технической меры, выбираемой на основе каких-либо предпочтений (цена, реализуемость и т. д). Наиболее часто используемым методом в последнем случае является защита с помощью паролей.

При реализации максимального класса защиты наблюдается стремление закрыть возможность доступа со всех прогнозируемых направлений, где может быть осуществлена атака на систему. Типичными мерами, включаемыми в "глухую защиту" являются: удаление клавиатуры у компьютеров и запрет сетевого доступа; наложение электронных замков, перемычек на электронные платы в контроллерах; использование механических ключей на шкафы автоматики и т.п.

Это эффективный и радикальный способ решения ЗНСД, однако он превращает программируемую технику АСУТП АЭС в непрограммируемую.

Парольный способ решения ЗНСД минимально ограничивает реактивность АСУТП АЭС при перенастраивании и адаптации к изменениям на эксплуатируемом объекте. Бытует мнение, что пароли должны обеспечить доступ к ПО со стороны людей, чей доступ разрешен, и оградить ПО от вмешательства со стороны посторонних, которые этого доступа не имеют. Но это не совсем так. Во-первых, пароли не защищают информацию от преднамеренного, но "ошибочного" доступа. Во-вторых, доступ к системе дается не конкретному человеку, а любому, кто знает пароль (т.е. не реализованы меры, обеспечивающие персонализацию

объекта, связанного с паролем). Это очень архаичный и ненадежный способ ЗНСД. Таким образом, даже поверхностный анализ указал на недостатки крайних подходов для решения ЗНСД АСУ ТП АЭС.

Оценить приведенные выше меры обеспечения ЗНСД можно путем рассмотрения угроз безопасности АСУТП АЭС со стороны различных групп пользователей. Выделим основные группы пользователей:

- разработчики знают все пароли, в том числе и системный, который открывает доступ ко всему ПО. Для них приемлема только глухая защита, а это означает, что их нельзя допускать на объект;
- наладчики также обязаны знать все пароли и тоже могут производить вредные модификации ПО. От них не спасет ни один из указанных выше способов;
- эксплуатационный персонал, который может быть существенно ограничен в своих действиях, если парольная защита выполнена надлежащим образом. Если при эксплуатации АСУТП необходимо производить ввод информации, настройку или иные действия над ПО, то парольная защита не будет обеспечивать ЗНСД;
- операторы-технологи – единственная группа персонала, для которой при помощи комбинации глухой защиты и паролей можно добиться хорошей ЗНСД;
- системные администраторы на практике выполняют всю совокупность функций обслуживания ПО АСУТП, включая его инсталляцию, настройку, модификацию и ЗНСД. По отношению к ПО они "всемогущи" и "бесконтрольны".

Таким образом, приведенные выше способы ЗНСД для АСУТП приходится признать неэффективными и недостаточными.

Объект и цели ЗНСД

Объектом ЗНСД является программно-технический комплекс АСУТП АЭС в целом, а не отдельные его составляющие (нижний уровень, верхний уровень, отдельные подсистемы АСУ ТП АЭС).

Целью ЗНСД является предотвращение и регистрация воздействий людей на ПО АСУТП АЭС, которые приводят к отказу функций АСУТП АЭС.

Под воздействием будем понимать любое действие человека по отношению к компоненте или АСУТП АЭС в целом. Санкционированное воздействие производится в силу служебных обязанностей либо по специальному распоряжению, несанкционированное – любое воздействие, которое не является санкционированным.

Задача ЗНСД сводится к определению факта и места воздействия; проверке, является ли оно санкционированным или нет; принятию мер по устранению вредных последствий в случае возникновения несанкционированного воздействия.

Очевидно, что эффективность любой системы ЗНСД зависит, в первую очередь, от того, насколько полно, точно и быстро будут определяться воздействия. Для ЗНСД АСУТП АЭС приемлема будет точность в пределах единиц и десятков секунд. Место воздействия необходимо определять с максимальной точностью до шкафа, приборной стойки, клеммной коробки и т.п.; необходимо фиксировать открытие дверей приборных стоек, подключение к разъемам ЛВС, входы в ОС и т.п.

Проверка на санкционированность должна проводиться на основе персонификации воздействия (для этого, в частности, применимы системы видеонаблюдения, реализованные на объекте) и использования средств ввода информации с фиксацией действия по изменению ПО.

Меры по устранению воздействий должны быть регламентированы на основе анализа возможных атак на безопасность системы.

Распределенная и централизованная модели ЗНСД

В современных АСУТП применяется в основном распределенная модель ЗНСД, в которой каждый элемент реализует свой комплекс мер по защите от НСД. Эта модель скопирована с офисных систем. Взлом одного компьютера здесь не затрагивает работу других. Поэтому система только слегка деградирует, а не выходит из строя. Если ее восстановят через сутки, ничего страшного не произойдет.

В системах АСУТП АЭС все элементы сильно связаны друг с другом. Поэтому порча одного элемента, например контроллера или сетевого коммутатора, может привести к отказу целого измерительного канала или множества каналов одновременно. Поэтому простои в течение суток недопустимы.

Альтернативой распределенной модели является предлагаемая централизованная модель системы ЗНСД. Здесь элементы АСУТП АЭС реализуют двухуровневую иерархическую систему ЗНСД. В первый, наиболее защищенный уровень входят все рабочие места операторов, используемые для управления АЭС. Для работы с ПО служат специализированные АРМ второго уровня (только с них возможно осуществить изменение ПО АСУТП АЭС), которые располагаются в охраняемых помещениях, где обеспечивается пропускной контроль и непрерывное видеонаблюдение за всеми сотрудниками. Персонал, работающий в этих помещениях, подразделяется на эксплуатационный, выполняющий работы по обслуживанию ПО АСУТП, и охранный, выполняющий функции ЗНСД.

В функции охранного персонала входят:

1) проверка нарушений физической защиты входов в АСУТП, включая открытие дверей приборных стоек, выемку модулей, подключение к ЛАН и т.п.;
2) непрерывный контроль за состоянием ПО;
3) проверка соответствия изменений ПО регламенту и нарядам на производство работ;
4) назначение паролей для входа в систему по принципу связанных пар "пароль-регламентная работа". Для каждой регламентированной операции с каждым компонентом ПО определяется свой пароль, т.е. осуществляется однозначное отображение элемента из

множества паролей на некоторое подмножество элементов из набора действий, определенных регламентом. При этом все прочие нерегламентированные действия должны быть заблокированы полностью. Не допускаются суперпароли, суперпользователи и т.п.

Централизованная модель имеет ряд преимуществ перед распределенной. Во-первых, она решает проблему допуска к ПО только нужных людей. Во-вторых, охранный персонал может непрерывно контролировать реализацию функций ЗНСД и принимать меры немедленно. В-третьих, разделение функций между эксплуатационным и охранным персоналом делает контролируемыми и безопасными работы по обслуживанию и изменению ПО АСУТП.

ЗНСД и жизненный цикл АСУТП АЭС

Разработка АСУТП АЭС включает следующие основные этапы: изготовление на заводе-изготовителе; пусконаладочные работы на объекте; эксплуатация. В ходе изготовления в АСУТП АЭС производится загрузка ПО и затем проводятся заводские испытания оборудования, в ходе которых выявляются дефекты, ПО дорабатывается, вновь загружается, проверяется и т.д. При этом часто возникает необходимость модификации уже тестированного ПО. Поэтому систему ЗНСД целесообразно устанавливать на заводе-изготовителе до начала проведения испытаний и фиксировать с ее помощью все изменения ПО.

В ходе проведения пусконаладочных работ система ЗСНД должна использоваться для автоматизированного контроля производимых изменений на объекте, где идет внедрение АСУТП АЭС, эксплуатироваться непрерывно и обеспечивать охранные функции. В ходе эксплуатации АСУТП АЭС система ЗСНД должна также функционировать непрерывно и обеспечивать, главным образом, охранные функции.

Анализ реализуемости предлагаемой модели централизованной системы ЗНСД

Является ли предложенная централизованная модель системы ЗНСД реализуемой? Современные ПЛК обладают развитой диагностикой, позволяющей сигнализировать о воздействии на них. Вычислительная техника и ОС с небольшими доработками способны точно сигнализировать о любых воздействиях со стороны людей. Проверка санкционированности воздействий также не представляет сложностей. Таким образом, создание централизованной системы ЗНСД вполне реально для любой современной АСУТП АЭС.

АСУТП АЭС "Бушер-1" имеет в своем составе подсистему, где логически концентрируются необходимые сигналы для обеспечения ЗНСД – это система верхнего блочного уровня. Поэтому в данном случае централизованная модель ЗНСД логически станет продолжением информационной модели АСУТП АЭС "Бушер-1" [3].

Заключение

Таким образом, создание эффективных централизованных систем ЗНСД для АСУТП АЭС является насущной необходимостью. Препятствием к этому служит лишь стереотип ЗНСД, заимствованный из области офисных вычислительных сетей, которые были внедрены раньше, чем АСУТП АЭС на основе программируемой логики.

Централизованные системы ЗНСД АСУТП АЭС должны создаваться на основе анализа угрозы НСД применительно ко всей системе, а не по отдельным ее компонентам. Необходимо анализировать угрозы, возникающие не только в процессе нормальной эксплуатации системы, а на всех этапах жизненного цикла, включая разработку и наладку.

Данные требования предполагается реализовать в системе ЗНСД, которую ИПУ РАН внедряет для АСУТП АЭС "Бушер-1" [4-5].

Список литературы

1. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.
2. ГОСТ Р 51241-98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.
3. BU.1 0.0.AT.TZ.PRR001. Автоматизированная система управления технологическими процессами (АСУ ТП). Техническое задание. Москва. 1998.
4. 00229530.51505.001.П2.3-1. Система верхнего уровня АСУТП атомной электростанции "Бушер-1" (СВБУ). Технический проект. Том 2. Пояснительная записка. Книга 1. Основные решения по системе и её подсистемам. Книга 3. Описание информационного обеспечения системы. ИПУ РАН. 2002.
5. Пояснительная записка по эскизно-техническому проекту создания системы информационной безопасности и защиты от несанкционированного доступа системы верхнего блочного уровня и СКУД. ПО "Старт". 1999 г.

Полетыкин А.Г. *– канд. техн. наук, старший научный сотрудник, зав. сектором 31.5,*
Промыслов В.Г. *– канд. физ.-мат. наук, старший научный сотрудник,*
Менгазетдинов Н.Э. *– зав. сектором лаб. 24 Института проблем Управления им. В.А. Трапезникова РАН.*
Контактные телефоны (095): 334-75-71, 334-25-22.

Безвентиляторное встраиваемое решение на ULV Celeron M 600МГц

Компания ИКОС объявила о начале поставок на российский рынок новой модели безвентиляторной встраиваемой процессорной платы Portwell, получившей название ROBO-6730VLA. Выполненная в формате платы PCI половинного размера, она продолжает линейку компактных одноплатных компьютеров Portwell. ROBO-6730VLA разработана на базе чипсета Intel 852GM со встроенным графическим ядром и поддержкой памяти DDR 200/266 и представляет собой платформу для создания на его базе Internet-приложений, мультимедийных систем, а также систем, требующих больших вычислительных мощностей.

http://www.icnews.ru