УДК 681.518.5

А. В. Карасевич, В. А. Руденко, В. Н. Безуб*

ПАО «ЕВРАЗ Днепропетровский металлургический завод им. Петровского», Днепропетровск
*Национальная металлургическая академия Украины, Днепропетровск

Совершенствование систем автоматического контроля и безопасности управления в АСУ ТП доменного производства

За последние 10 лет проектные институты и инжиниринговые компании научились проектировать базовые автоматизированные системы управления технологическим процессом (АСУ ТП) в стандартном функционале. Основная информация, циркулирующая в системах технологического управления – это информация о технологических процессах и управляющих воздействиях. Обладание этой информацией без физического доступа к объекту управления не даёт возможности совершить кражу, что резко ограничивает круг потенциальных нарушителей. Риски, связанные с мошенническими операциями в АСУ ТП, можно ограничить действиями внутреннего нарушителя – собственного персонала компании или компаний-партнеров. К примеру, для реализации схем с модификацией данных по расходу топлива на автозаправке надо иметь возможность слива и реализации этого топлива.

Ключевые слова: *автоматизированные системы управления, информационная целостность, контроль целостности систем управления*

Постановка проблемы. Из опыта эксплуатации средств АСУ ТП на различных предприятиях можно сделать вывод об отсутствии действительно эффективных многоуровневых систем защиты в большинстве случаев. В некоторых случаях были замечены попытки решить проблемы безопасности самим обслуживающим персоналом с помощью стандартных средств, но подобные решения оставляют желать лучшего.

Когда проблемами безопасности занимаются неспециалисты в области безопасности или небольшой круг энтузиастов, они исходят из имеющегося у них опыта, при этом устраняя одни проблемы и создавая другие.

Постановка задачи. Появилась необходимость создания системы безопасности в автоматизации, которая должна базироваться на безопасном выполнении поставленных перед технологическим персоналом задач, а также на максимально возможном воспрепятствовании возникновению аварийных ситуаций. Решение подобных задач позволит выявить потенциальные риски в комплексах АСУ ТП с помощью системы диагностики и контроля, которая сможет обеспечить исправное состояние ключевых узлов, и поможет уменьшить влияние человеческого фактора.

Анализ последних исследований и публикаций. Наиболее распространённые угрозы безопасности связаны с монетизацией киберпреступности, то есть с получением денежной выгоды от реализации тех или иных атак на инфраструктуру предприятия, промышленным шпионажем и в редких случаях – шантажом и заказными акциями против конкурентов. Несмотря на это, АСУ ТП до последнего времени не являлись привлекательными для потенциального внешнего нарушителя. Остальные инциденты являются немонетизируемыми: месть уволенных работников, нарушение функционирования вредоносным кодом, случайные взломы хакерами.

Из вышеописанного следует – количество публично известных нарушений функционирования подобных систем крайне невелико. Кроме того, в случае серьёзных нарушений функционирования процессов, контролируемых системой управления, борьба с последствиями не будет отличаться от борьбы с техногенной аварией. Системы технологического управления рассчитываются на быстрое восстановление после сбоев как в случае автоматизации, так и без неё.

Однако низкая вероятность внешних атак на системы АСУ ТП не снижает актуальность угроз для систем управления. Согласно общепринятой практике, актуальность угрозы пропорциональна как вероятности реализации угрозы, так и возможному ущербу от её реализации, а если говорить о возможном ущербе от реализации угрозы, тогда системы управления, особенно системы управления опасными производственными циклами или системы жизнеобеспечения целых городов и областей, будут вне конкуренции.

Возможный ущерб от реализации подобных атак включает, кроме финансовых потерь, риски репутационные и связанные с потерей здоровья и жизни, а также риски возникновения экологических катастроф. Даже единичное нарушение функционирования систем технологического управления может привести к катастрофическим последствиям. Подобные инциденты в системах технологического управления, при их обнародовании, вызывают большой общественный резонанс.

По причине практически отсутствующей огласки про нечастые случаи кражи конфиденциальной информации или возникновение специализированных вирусов, способных создать аварийную ситуацию на производстве, компании, проектирующие комплексы АСУ ТП для промышленных предприятий, часто не заботятся о создании мер безопасности производства и контроле целостности информации. Некоторые компании-разработчики средств

автоматизации создают отдельные компоненты, повышающие уровень контроля и безопасности, но охватить все потенциальные варианты задач практически невозможно. Также значительную роль играет неведение заказчика относительно всех возможностей средств автоматизации, что только усугубляет ситуацию.

Например, одним из громких и резонансных инцидентов, показывающий уязвимость и возможность эксплуатации данной уязвимости сетей управления на практике, стал обнаруженный в июле 2010 г. вирусный код Stuxnet, который фактически является первым в истории вирусом, способным портить не только данные и программный код, но и вполне реальные машины и оборудование. Его возникновение не только выявило очередные уязвимости в операционных системах Microsoft, но и устремило взоры специалистов по информационной безопасности в абсолютно новую для них область – безопасность промышленных систем. Способ распространения, направленность и деятельность внедрённого в промышленность вируса говорит о специализации вируса на крупные промышленные и стратегические объекты.

Ниже (таб. 1) приведены основные факторы, влияющие на уязвимость действующих систем по тем или иным причинам.

Изложение основных материалов исследований. В настоящий момент для унификации и типизации процессов и технологий существует целый ряд стандартов и рекомендаций. Заслуживают внимания, тщательного анализа и рекомендации производителей. Одним из примеров таких практических рекомендаций может быть руководство по проектированию и внедрению конвергированной Ethernet сети предприятия (Converged Plantwide Ethernet Designand Implementation Guide), разработанное компаниями Cisco и RockwellAutomation. Назначение этого документа – определение эталонных сетевых архитектур, ориентированных на применение производственными предприятиями и облегчающих объединение промышленных и корпоративных сетей с учётом требований по безопасности.

В настоящее время, инфраструктура ПАО «ЕВРАЗ – ДМЗ им. Петровского» также нуждалась в доработке своей системы безопасности. В первую очередь – обезопасить существующие системы автоматизации от человеческого фактора, то есть от случайного или намеренного воздействия обслуживающего персонала, действия которого могут привести к трагическим последствиям или техногенным катастрофам. Подобными и другими вопросами промышленной безопасности существующих автоматизированных систем в доменном цехе последние четыре года активно занимаются специалисты отдела эксплуатации АСУ ТП при содействии научных работников Днепропетровской металлургической академии.

На рисунке приведён достигнутый результат – многоуровневая система защиты и контроля.

Немаловажную роль необходимо отводить поддержке используемого программного обеспечения, а именно: своевременному обновлению операционных систем, технологического и промышленного ПО; запрету на использование нелегальных приложений и применению антивирусных программ. В настоящий момент уже прекращена поддержка таких распространённых операционных систем, как Windows XP и Windows 7. Поэтому, в целях безопасности, необходимо рассмотреть переход на ОС нового поколения, поддерживаемые и обновляемые разработчиком. Этот вопрос касается и программного обеспечения

Таблица 1

Основные факторы влияния на уязвимость действующих систем

Большое количество «собственных» разработок программно-аппаратных решений при создании АСУ ТП	
длительный срок эксплуатации систем	
Закрытость систем	разработка в расчёте, на выполнение в доверенной среде закрытых индустриальных сетей; использование специализированных протоколов и средств связи, а также часто низкая скорость их роботы; отсутствие ревизий систем и кода на безопасность; разработка без учёта лучших практик разработки безопасного кода;
Фиксированные конфигурации	отсутствие возможности своевременного обновления ПО и установки последних исправлений безопасности; отсутствие возможности установки наложенных средств безопасности (например, антивирусного ПО) и их своевременного обновления; использование паролей и настроек безопасности по умолчанию, включая настоятельные рекомендации производителя не менять данные значения;
Производительность	системы технологического управления оперируют информацией в реальном времени, дополнительные проверки систем безопасности мешают;
Открытые стандарты	новое поколение систем технологического управления работает на открытых стандартах (прежде всего протоколы TCP/IP). При этом, даже в случае разделения сетей (технологической, офисной, сети интернет) связи сохраняются для технологических нужд (пересылка информации, удаленное управление).
Консервативный подход к проблемам безопасности (заключающийся, как правило, в периметровой защите и разделении сетей). Возможности управления доступом в рамках прикладных систем ограничены.	
Информация (технологическая) не является основным объектом защиты систем, часто не является конфиденциальной.	
Основной объект защиты – управляющее воздействие.	

Многоуровневая система защиты и контроля

верхнего уровня – средств программирования промышленных контроллеров и SCADA-системы, в последних версиях которых уделено много внимания вопросам безопасности и защиты информации, разграничениям прав действий и функций пользователей и их тщательной настройке.

Следующим этапом необходимо обеспечить внутреннюю безопасность системы, а именно контроль и анализ действий технологического и обслуживающего персонала. На ПАО «ЕВРАЗ – ДМЗ им. Петровского» уже реализована и функционирует в течение нескольких лет подсистема аудита верхнего и нижнего уровней, фиксирующая все действия персонала, с помощью которой возможно выяснить, кто, когда и каким образом выполнял изменения в системе нижнего и верхнего уровней, начиная от подключений к серверу визуализации и заканчивая изменениями, вносимыми в логические контроллеры. Подсистема аудита, функционирующая немногим более трёх лет, уже успела доказать свою эффективность, позволив выявить несоответствия между регистрацией действий самим дежурным персоналом с фактически выполняемыми изменениями. К тому же использование аудита изменений позволяет выявить сотрудников, выполнивших неквалифицированные действия, которые, в иных случаях, могли привести к необратимым последствиям.

Большую роль в технологическом процессе играет и подсистема сигнализаций. С её помощью технологический персонал может увидеть сообщаемые системой АСУ ТП отклонения в своей работе и немедленно принять соответствующие меры по восстановлению штатного функционирования. Сообщения имеют вид всплывающих окон или мерцающих надписей, и представляющих в графическом виде узел системы, в котором произошло отклонение заданных параметров, позволяя персоналу быстро определить значимость проблемы и необходимости вызова соответствующей службы для её устранения. Одновременно с этим присутствует сводка всех поступающих аварийных сообщений, которые будут отображаться до момента подтверждения их просмотра.

Ввиду того, что доменное производство сопряжено с определёнными рисками возникновения критических ситуаций, множество узлов и механизмов системы оснащено блокировками, выполняющими функции аварийной остановки работы части системы. К таким объектам можно отнести баллоны, работающие под давлением, трассы доменного и природного газов и другие объекты, способные создать угрозу катастрофического или техногенного характера. Для отслеживания и анализа сработавших блокировок технологическому персоналу предоставляется отчёт в виде таблицы с количеством срабатываний и значениями параметров.

Одна из подсистем, внедрённых в АСУ ТП в последнее время, является подсистема контроля логических цепей ПЛК, и направлена на анализ работы механизмов в нижнем уровне, то есть на уровне логических контроллеров, и призвана повысить контроль над последовательностью возникновения неисправностей логических цепей. В комплексах АСУ ТП описывают различные узлы системы в основном с помощью языка программирования LadderDiagram, представляющим собой набор логических сигналов, объединённых в общую цепь, и имеющих на выходе цепи-результаты конъюнкции и дизъюнкции этих сигналов. Простейшими элементами языка являются контакторы, которые можно образно уподобить контактам реле или кнопки. Контакты отождествляются с переменными, а состояние контакта является значением переменной. Результат на выходе определяет управляющие сигналы для работы механизмов, разрешение и запрет на их работу, согласованную работу всех механизмов системы в целом.

Диагностика состояния логических цепей затруднена, поскольку цепь отображает только текущее состояние, и определить её предыдущее состояние, например причину отключения, не представляется возможным. Данная подсистема позволяет отследить последовательность отключения сигналов цепи, и оперативно выявить истинную причину некорректной работы ключевых логических

цепей, наглядно представляя изменение состояния цепи в разные промежутки времени. Все изменения наблюдаемых цепей записываются в систему длительного хранения данных, позволяя накапливать статистическую информацию и выявлять тенденцию нарушенной работы устройств.

В целом, приведён перечень мероприятий, который должен стать базовым стандартом (табл. 2).

Таблица 2

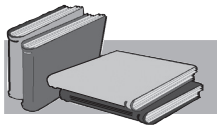
Базовый перечень мероприятий

Предотвращение ошибок персонала	Предотвращение преднамеренных («хулиганских») действий сотрудников
формирование требований по защите информации в процессе разработки и внедрения систем АСУ ТП; организация мониторинга действий персонала и состояния критичных компонентов АСУ ТП; проведение обязательного повышения квалификации персонала, занятого обслуживанием АСУ ТП; тщательный подбор и подготовка персонала для решения поставленных задач, включая личную ответственность за совершаемые действия.	ограничение полномочий пользователей в использовании программной среды АСУ ТП рамками их должностных обязанностей; контроль роботы с переносными устройствами и устройствами ввода/вывода; применение строгой аутентификации при доступе к программной среде АСУ ТП; формирование строгой антивирусной политики и повсеместное применение средств антивирусной защиты; проведение регулярных инструктажей об ответственности, возложенной на сотрудников, занятых в эксплуатации ключевых компонент АСУ ТП; резервное копирование ключевых компонентов АСУ ТП и средств, задействованных в обеспечении их безопасности; автоматизированный мониторинг состояния защищенности ЛВС АСУ ТП.

Выводы

Автоматизированные и автоматические системы технологического управления прочно интегрированы в наш социум. Их функционирование может затрагивать не только интересы отдельных промышленных компаний, эксплуатирующих подобные системы, но иногда – всех и каждого. Вероятность атаки на подобные системы ниже, чем на многие другие, но ответственность, связанная с их защитой, в некоторых случаях несоизмеримо выше.

Когда дело доходит до внедрения, в большинстве случаев меры безопасности начинаются и заканчиваются на границе между технологическим и корпоративным сегментами ЛВС. Но чтобы противодействовать современным угрозам в сфере АСУ ТП, недостаточно поставить межсетевой экран на границе и установить на серверах и АРМ антивирусную программу. Нужно применять технологии безопасности ниже, внутри АСУ ТП, на уровне серверов, ПЛК, интеллектуальных датчиков и исполнительных механизмов. Экономический эффект от внедрения систем безопасности будет достигаться за счёт снижения простоев агрегатов, возможности ретроспективного анализа причин сбоев в работе оборудования, а также снижения расхода человеческих ресурсов на восстановление хронологии аварийных ситуаций. Кроме того, дальнейшее развитие систем безопасности позволит значительно эффективнее выявлять проблемные узлы в комплексах промышленного оборудования, и таким образом повышать общий показатель экономической эффективности предприятия.



ЛИТЕРАТУРА

1. *Нестеров А. Л.* Проектирование АСУ ТП. Методическое пособие / А. Л. Нестеров. – Изд-во «ДЕАН», 2006. – Кн. 1. – 552 с.
2. *Нестеров А. Л.* Проектирование АСУ ТП. Методическое пособие / А. Л. Нестеров. – Изд-во «ДЕАН», 2009. – Кн. 2. – 944 с.
3. *Федоров Ю. Н.* Справочник инженера по АСУ ТП: проектирование и разработка / Ю. Н. Федоров. – М.: Инфра-Инженерия, 2008. – 928 с.
4. *Гарбук С. В.* Обзор информационной безопасности АСУ ТП зарубежных государств. Гарбук Сергей Владимирович, Комаров Андрей Андреевич, Салов Евгений Игоревич (http://www.securitylab.ru/analytics/398184.php).
5. Безопасность АСУ ТП и контроль привилегированных пользователей (http://www.anti-malware.ru/node/11899).
6. *Волобуев П.* Практическая демонстрация типовых атак и 0-day уязвимостей в SCADA и PLC-контроллера / П. Волобуев, А. Миноженко, А. Поляков. – DigitalSecurity, 2011 г.
7. *Ницель Ли.* 6 шагов к информационной безопасности АСУ ТП / Ли Ницель (http://ua.automation.com/content/6-shagov-k-informacionnoj-bezopasnosti-asu-tp).

Анотація

Карасевич А. В., Руденко В. А., Безуб В. Н.

Вдосконалення систем автоматичного контролю та безпеки керування в АСУ ТП доменного виробництва

За останні 10 років проектні інститути та інжинірингові компанії навчилися проектувати базові автоматизовані системи управління технологічним процесом (АСУ ТП) у стандартному функціоналі. Основна інформація, яка циркулює в системах технологічного управління – це інформація про технологічні процеси і керуючі впливи. Володіння цією інформацією без фізичного доступу до об'єкта управління не дає можливості вчинити крадіжку, що різко обмежує коло потенційних порушників. Ризики, пов'язані з шахрайськими операціями в АСУ ТП, можна обмежити діями внутрішнього порушника – власного персоналу компанії або компаній-партнерів. Наприклад, для реалізації схем з модифікацією даних по витраті палива на автозаправці треба мати можливість зливу і реалізації цього пального.

Ключові слова

автоматизовані системи управління, інформаційна цілісність, контроль цілісності систем управления

Summary

Karasevich A. , Rudenko V., Bezub V.

Improvement of automatic control systems and safety management in process control domain of production

Over the past 10 years, design institutes and engineering companies have learned how to design a basic automated control system of technological process (ACS TP) in the standard functionality. Basic information circulating in the control systems technology is the information about technological processes and control actions. The possession of this information without physical access to the object of control does not allow to commit theft, which drastically limits the number of potential violators. Risks associated with fraudulent transactions in process control, you can restrict the internal action of the offender is a private company staff and partner companies. For example, to implement schemes with a modification of data on fuel consumption at the gas station should be able drain and implementation of this fuel.

Keywords

automated control systems, information integrity, control of integrity of control systems

Поступила 20.04.2015