зультат расчета вносится некоторая доля произвола, искажающая требуемое качество работы системы.

Следует отметить также частый недостаток внедрения системы, снижающий конкретность анализа работы производства: из-за недостаточно точной и достоверной работы имеющихся расходомеров на многих путепроводах и/или из-за отсутствия расходомеров на них (вместо их установки, замены, модернизации), общее сведение баланса проводится по учету изменения материала в хранилищах производства за заданный интервал времени. Это исключает детальный учет движения материала по производству, не позволяет анализировать согласование баланса по отдельным технологическим агрегатам, мешает точному выявлению мест возникновения сверхнормативных потерь.

Список литературы

1. *Козин В.Г.* Разработка поточной схемы и расчёт товарного баланса нефтеперерабатывающего завода: Методические указания. Казанский государственный технологический университет. Казань. 1993.
2. *Грошева Л.П.* Основы материального баланса. Методическое пособие. Новгородский государственный университет. 2006.
3. Система сведения материального баланса предприятия *на базе продукта PI SigmaFine. http://www.mcee.runmcee.runmx.mcee.ru/print.php?id=247.*

Гребенюк Елена Алексеевна *– д-р техн. наук, ведущий научный сотрудник,*
Ицкович Эммануил Львович *– д-р техн. наук, проф., зав. лабораторией ИПУ им. В.А. Трапезникова РАН.*
Контактный телефон (495) 334-90-21.

Обеспечение безопасности АСУТП промышленного предприятия

И.В. Лопухов (Компания Прософт)

Сегодня в промышленных системах управления наблюдается постепенный переход средств управления на стандарт Ethernet. При этом появляется специфическое промышленное вредоносное ПО, направленное на отдельные типы промышленных систем управления. О принципах противодействия и защиты сети промышленного предприятия от существующих и потенциальных угроз согласно стандартам ANSI / ISA-99 рассказывается в данной статье.

Ключевые слова: кибер-атаки, вирусы, межсетевой экран, виртуальные сети, безопасность, источники угроз, сегментация сети.

Анализ уязвимости современных систем АСУТП

В процессе слияния корпоративных сетей передачи данных с АСУТП возникла тенденция замены промышленных сетей и сетей с собственными узкоспециализированными протоколами передачи данных доступным коммерческим оборудованием, использующим Ethernet TCP/IP технологии. С одной стороны, Ethernet сеть, пронизывающая насквозь все уровни предприятия — это гибкое и удобное информационное пространство, позволяющее вывести процессы автоматизации на новый уровень, с другой — вредоносное ПО нового типа теперь может вмешаться в производственный процесс и причинить крупный урон деятельности предприятия. ПЛК и прочие средства управления полевого уровня вместе с подключением к Ethernet стали открыты новым источникам угроз, на которые их разработчики не рассчитывали. В результате серьезно возросло число сбоев и простоев оборудования из-за последствий вредоносного ПО и кибер-атак [1].

Анализ крупнейшей в мире БД по инцидентам в сфере безопасности SCADA-систем и АСУТП www.securityincidents.org (RISI, Repository for Industrial Security Incidents) за период 1982–2010 гг. показал, что сбои в работе систем управления вызываются следующими факторами:

— 50% инцидентов произошли случайно;

— 30% были вызваны вредоносным ПО;

— 11% случаев произошли «благодаря» несанкционированному доступу извне;

— 9% инцидентов произошло из-за вредоносных действий изнутри.

Выделим три основных источника проблем безопасности.

1) *Уязвимости в программной части оборудования.* SCADA-системы и средства АСУТП, такие как ПЛК, удаленные терминалы и интеллектуальные конечные устройства, проектировались из расчета максимальной надежности и возможности ввода/вывода в реальном времени. Вопроса защищенного обмена данными по сети практически не существовало. Некоторые средства полевого управления перестают нормально функционировать при получении по сети нестандартных посылок данных или чрезмерного потока данных правильного формата. Также ПК под управлением ОС Windows в сетях управления традиционно работают без обновлений системы, «патчей» и антивирусных баз, что делает их уязвимыми даже для устаревших типов вредоносного ПО.

2) *Множественные точки входа.* Даже без прямого подключения к сети Internet современные системы управления доступны из множества внешних ресурсов, с которых возможна потенциальная атака. К источника потенциальной опасности относятся: интерфейсы удаленного управления и диагностики, серверы MES, модемы удаленного доступа, последовательные соединения, беспроводные системы, мобильные станции оператора, USB-накопители, файлы данных о процессе, файлы документации (PDF).

Данные способы доступа к системам управления обычно не принимаются во внимание руководством предприятий. Кроме того, они плохо задокументированы.

Специалисты исследовательского центра NCCIC (National Communication Integration Center) в среднем насчитывают 11 способов доступа к закрытому контуру сети АСУТП, который закрыт от общей сети предприятия. В отсутствии строгой политики разграничения сети производственного участка от корпоративной сети прямых способов подключения к промышленному контуру может быть до 250 вариантов. Анализ атак вируса Stuxnet в 2010 г. подтверждает, что все открытые каналы доступа к промышленному сегменту сети могут быть задействованы вредоносным ПО.

3) *Недостаточная сегментация сети*. Сети передачи данных в АСУТП сейчас намного более сложны, чем раньше. Они объединяют сотни, а иногда и тысячи конечных устройств. К сожалению, данные сети в основном являются «плоскими», сегментация практически отсутствует. В результате проблемы, возникшие на одном участке сети, быстро распространяются на всю сеть.

Построение сети связи предприятия с учетом стандарта ANSI/ISA99

Большинство компаний, решающих задачу автоматизации и модернизации производства, сталкиваются с проблемой доступа к данным и совместного их использования разными подсистемами и приложениями. В этой реалии задачи по ограничению связей и доступа к отдельным сегментам фактически находятся в противофазе с основной производственной потребностью в информации. Более того, современные технологии требуют открытого доступа к данным уровня автоматизации и полевого уровня. Часто обмен данными протекает в форме установки обновлений, «патчей», «прошивок», подключений для удаленного управления. Все эти процессы несут потенциальную угрозу безопасности сети.

У инженеров, работающих с АСУТП и SCADA-системами, весьма ограниченные возможности по борьбе с уязвимостями программных компонентов. Агрессивная политика постоянного обновления программных средств позволяет снизить потенциальную угрозу, исходящую от вредоносного ПО. Однако такая политика не пользуется успехом у операторов систем, в значительной степени зависимых от производителей аппаратных средств автоматизации, например ПЛК. Отданные на откуп производителям компонентов автоматизации проблемы безопасности фактически не решаются. В конце 2011 г. комитет US ICS-CERT (www.Us-cert.gov) опубликовал результаты исследований 137 продуктов промышленной автоматизации со списками выявленных уязвимостей в их безопасности. Менее 50% из них позже получили доступные обновления безопасности.

Система стандартов ANSI/ISA-99 — это комплексная программа повышения уровня безопасности промышленных систем автоматизации и управления. Она содержит 11 стандартов и технических отчетов, опубликованных Американским Институтом стандартов (ANSI — American National Standards Institute). Комитет ISA-99, отвечающий за разработку стандартов, входит в Международную техническую комиссию (IEC — International Electrotechnical Commission), разрабатывающую общий стандарт по промышленной безопасности IEC 62443: Industrial network and system security.

Стандарт ANSI/ISA-99 предлагает концепцию «зон» и «каналов» для сегментации и изоляции участков и подсистем общей системы управления. «Зоной» называется объединение логических или физических средств, для которых предъявляются схожие требования по безопасности, таких как критичность для ТП. Оборудование в каждой зоне получает определенный уровень безопасности. Как правило, встроенные средства безопасности не удовлетворяют выбранному уровню, поэтому внутри зоны применяются дополнительные средства и политики, повышающие безопасность.

Весь обмен данными между зонами должен быть взят под контроль и проходить только по определенным каналам связи. Отслеживание и анализ трафика, проходящего по выделенным каналам, помогает предотвращать DoS-атаки (Denial of Service), распространение вредоносного ПО, защитить соседние зоны, целостность и конфиденциальность трафика. В общем, контроль каналов связи между зонами призван смягчить разницу между уровнями безопасности и требованиями. Обеспечение контроля таких каналов — гораздо менее затратное мероприятие, чем модернизация каждого элемента внутри зоны до соответствия заявленному уровню безопасности.

Важно понимать, что система стандартов ANSI/ISA-99 не определяет конкретных методов или алгоритмов выделения зон и каналов внутри сети передачи данных предприятия. Стандарты предлагают набор требований по обеспечению безопасности в зависимости от уровня рисков компании быть подвергнутой кибер-атакам. Риски заключаются не столько в возможности кибер-атаки, сколько в ее последствиях, уменьшение которых достигается за счет локали-

Таблица. Ключевые требования к зонам и каналам передачи данных из стандарта ANSI / ISA-99.02.01.

Номер подраздела и краткое описание	Требования
4.3.2.3.1. Разработка архитектуры сегментированной сети передачи данных	Конечные сетевые устройства классифицируются в соответствии с рекомендациями IASC (International Association of Classification Societies), каждый класс в зависимости от уровня потенциальной опасности выделяется в отдельную защищенную зону.
4.3.2.3.2. Изоляция и сегментация оборудования с наиболее высоким уровнем риска	Зоны с максимальным уровнем риска должны быть изолированы с помощью специальных барьерных устройств от других зон, имеющих отличный уровень или иные политики безопасности. Барьерные устройства подбираются в соответствии с необходимым уровнем безопасности.
4.3.2.3.3. Блокировка всех неиспользуемых каналов связи между зонами	Барьерные устройства призваны блокировать весь неразрешенный трафик сети как внутрь, так и из защищенной зоны, содержащей критически-важное оборудование.

зации вредоносных воздействий в выделенной зоне, максимально изолированной от остальных.

Таблица предлагает перечень основных разделов стандарта ANSI/ISA-99.02.01, относящихся к сегментации сети на зоны и выделению каналов связи между ними.

Основание защищенных зон внутри сети

Сегментирование сети, выделение безопасных зон и каналов связи между ними начинается с группирования оборудования по принципу схожей функциональности или требований по безопасности. Выделенные группы оборудования становятся зонами, для которых устанавливается определенный уровень защиты.

Например, аппаратные средства на первом этапе могут быть разделены на производственные зоны, такие как складские средства автоматики, средства АСУ основного ТП, средства финишной обработки продукции и т. п. Затем внутри этих областей возможна дальнейшая сегментация по функциональным уровням. Иногда выделяются зоны с оборудованием, реализующим определенный стандарт (МЭК 61850), или согласно рекомендациям производителя оборудования.

Каждая зона определяется набором атрибутов и характеристик, включая: характеристики зоны (название зоны, определение, функциональная направленность); границы зоны; типовое оборудование (в идеале, перечень); изоляция от остальных зон; оценка рисков в пределах зоны (возможности по обеспечению безопасности для оборудования внутри зоны, угрозы и уязвимости, последствия от возникновения «дыр» в системе безопасности, возможный ущерб от кибер-атак); цели обеспечения безопасности; стратегии обеспечения безопасности; применение новых политик; обмен данными между зонами (требования к доступу); модификация системы управления в соответствии с предыдущими изменениями.

Каждая зона определяется не только границами, набором средств автоматизации и анализом рисков, но и возможностями по обеспечению безопасности. Например, возможности по обеспечению безопасности в зоне, где используются серверы под управлением ОС Windows 2008 Server, серьезно отличаются от зоны, где используется, например, Windows NT или ПЛК. Различия в возможностях и в уровнях потенциальных угроз рождают разные требования к системам безопасности самих зон и каналов связи между ними. Определить требования и потенциальные возможности по обеспечению безопасности поможет стандарт ISA-62443.03.03 — «Безопасность для систем автоматизации и управления: Требования к безопасности систем и уровни обеспечения безопасности» [2].

Зоны также могут выделяться в соответствии с набором управляющего оборудования. Так, ПЛК старого образца имеют более слабые механизмы авторизации, поэтому могут быть выделены в отдельную зону, где будут добавлены необходимые функции проверки пользователей.

Выделение безопасных каналов связи между защищенными зонами

После сегментирования сети передачи данных на зоны, следующим этапом является выделение связей между зонами, в терминологии стандарта — «каналов». Каждый канал определен согласно зонам, которые он соединяет, технологиям, которые используются для связи между зонами, протоколам передачи данных и функциям безопасности, используемым в зонах. Трафик, проходящий по таким каналам обычно детально известен. Для этого применяются утилиты-анализаторы трафика и анализаторы протоколов, они дают достаточно полную информацию об обмене данными и сервисах, использующих канал.

Также полезно заглянуть «за» сеть, выделить скрытое перемещение данных: передаются ли файлы между инженерной лабораторией и охраняемой зоной на USB-носителях; случаются ли удаленные подключения к терминалам внутри зоны через модем? Такие «мелочи» легко упустить из расчета, но вместе с тем они образуют серьезную брешь в безопасности при отсутствии внимания к ним.

Диаграмма движения данных (рис. 1) — отличный инструмент для учета данных в зонах и каналах между ними. Каждая зона может обозначаться точкой, а движение определенных данных — вектором.

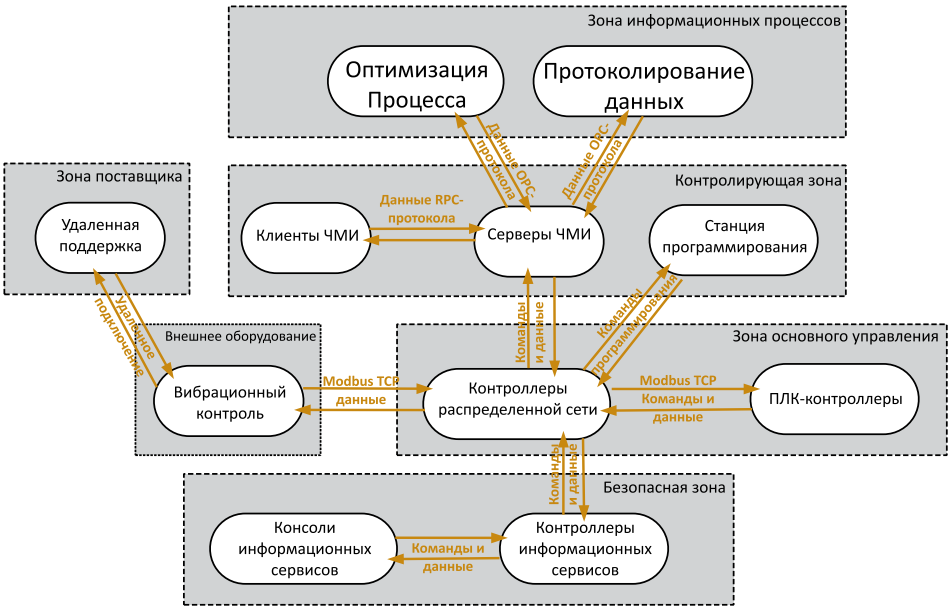

Рис. 1. Пример диаграммы движения данных

Способы защиты каналов связи

Как только каналы связи выделены, и требования по обеспечению безопасности определены, можно применять технологии по обеспечению безопасности. Назовем две наиболее известные.

— *Межсетевые экраны* — это граничные устройства, контролирующие и инспектирующие трафик в/из зоны. Они сравнивают проходящий через них трафик с заранее заложенными в них политиками безопасности, все пакеты данных, не относящиеся к разрешенному типу, удаляются. Обычно они конфигурируются на пропуск минимального объема данных, достаточного для корректной работы всей системы. Особое внимание должно уделяться трафику с высоким уровнем риска, таким как команды программирования ПЛК или некорректно-сформированные пакеты данных, которые могут использоваться для взлома системы. Отличие специальных промышленных межсетевых экранов здесь будут очевидны: они проектируются больше для инженеров АСУТП, чем для ИТ-специалистов и в соответствии с потребностями в АСУТП. Имеются возможности глубокого анализа протоколов, используемых в SCADA — системах, таких как DNP3, Ethernet/IP, ModBus TCP.

— *Сети VPN или виртуальные сети* — это зашифрованные логические каналы связи, существующие поверх физической сети и реализующие приватную передачу данных и команд. Сессию VPN называют «тоннелями», они реализуются на третьем «транспортном» уровне модели OSI. Приватные данные передаются вложенными в специальные пакеты данных, видимые только зарегистрированным пользователям. Присоединение к сети VPN осуществляется посредством специальных электронных ключей и сертификатов.

Комплексная защита зон и каналов связи возможна только при реализации технологий защиты на всех уровнях сети от физического до прикладного, что невозможно без совместной работы специалистов АСУТП и ИТ.

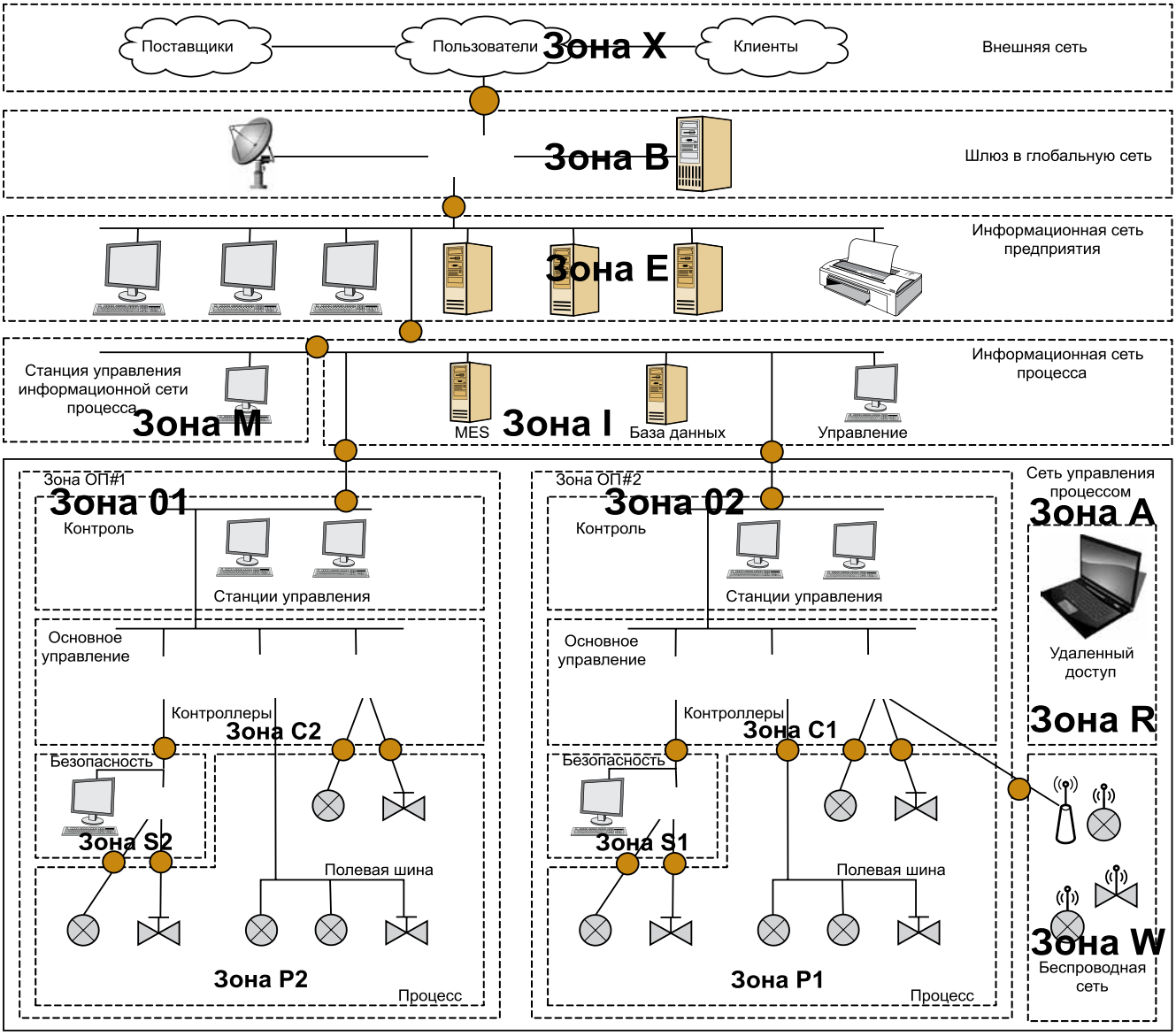

Рис. 2. Диаграмма зон и путей передачи данных на нефтеперегонном заводе

Пример разделения сети на сегменты

Рассмотрим две производственные области большого нефтеперегонного завода, на котором присутствуют ТП дистилляции, гидроочистки, каталитического реформинга, заготовки и пр.

Разделим производственный процесс на зоны по функционалу, по уровням процессов, по требованиям безопасности. Все функции управления принадлежат зоне управления процессом (Зона А на рис. 2). Внутри зоны А выделено несколько рабочих зон (О1, О2 и т. д.) на каждую значимую рабочую единицу. Уровень требований безопасности для каждой зоны может варьироваться. Например, потенциальный риск для системы управления процессом гидрокрекинга выше, чем в случае с процессом водоочистки.

Для каждой выделенной зоны необходимо составить список атрибутов. Этот процесс носит интерактивный характер, на этапе описания зоны ее границы могут быть изменены и выделены новые зоны.

Пример написания атрибутов зоны S1 представлен на вставке.

В приведенном примере инженеры нефтеперегонного завода провели анализ системы на предмет выделения потенциальных источников угроз, оценку их возможных последствий. Из анализа системы стало ясно, что систему безопасности на каждом производственном участке необходимо выделить в отдельную зону (изначально она была объединена с зоной системы базового управления). Для безопасного функционирования завода функции безопасности каждого процесса должны быть отделены от сети управления заводом.

Имея определенные зоны, можно переходить к определению путей сообщения между ними. На рис. 2 они отмечены коричневыми кругами. Под термин «путь» здесь попадают все информационные каналы между двумя зонами: не только сетевые подключения, но и перенос данных на съемных носителях и пр.

Реализация защиты сети по стандарту ISA-99 с помощью промышленных межсетевых экранов

Последняя стадия обеспечения безопасности зон и путей — выбор средств защиты. Существуют специализированные средства обеспечения технологии «защиты в глубину» для промышленных сетей управления. Например, интегрированный модульный аппаратно-программный комплекс Hirschmann Eagle Tofino, предназначенный для создания безопасных зон внутри информационной сети предприятия.

Устройство Eagle Tofino изначально предназначено для интеграции в существующую сеть. Режим «по-умолчанию» у межсетевого экрана — прозрачный. Таким образом, устройство интегрируются в сеть без каких-либо изменений в топологию или адресное пространство. Оно может быть детально настроено под конкретные задачи, на него могут быть установлены программные компоненты, реализующие такие функции, как файрвол, VPN клиент/сервер, глубокий мониторинг конкретных протоколов передачи данных (Modbus или OPC).

Пример заполнения атрибутов Зоны S1

Название: Участок 1. Система безопасности гидрокрекинга.
Определение зоны: зона включает все системы обеспечения безопасности гидрокрекинга
Контролирующая организация: Отдел АСУТП.
Основная функция зоны: обеспечение безопасности Участка 1 гидрокрекинга.
Границы зоны: соответствует участку 1.
Типовой набор средств: интегрированный системный контроллер безопасности, станция инженера АСУ, коммуникационное оборудование.
Наследование: зона наследует атрибуты от Зоны С1 (базовая система управления участка 1)
Оценка уровня риска: зона с уровнем риска от низкого до умеренного, но с чрезвычайно серьезными последствиями в случае взлома

a) Средства безопасности зоны. Оборудование способно противодействовать атакам низкого уровня подготовки (инициированным непрофессиональными хакерами или неспециализированным вредоносным ПО), направленным на доступность оборудования или конфиденциальность данных. А также атакам среднего уровня, направленным на нарушение целостности системы.
b) Угрозы и уязвимости. Уязвимости таких зон являются типовыми для существующих промышленных систем управления, использующих протокол Modbus для коммуникаций. Основные типы угроз:
   a. DoS (Denial of Service) — атаки, направленные на вывод из строя системы коммуникаций;
   b. внутренний или внешний несанкционированный доступ на рабочую станцию;
   c. считывание команд управления Modbus/TCP;
   d. считывание ответов системы на посылку Modbus/TCP команд;
   e. перепрограммирование функций безопасности
c) Последствия взлома системы безопасности:
   a. отказ работы системы на ⩾ 6 ч из-за ошибочного или аварийного завершения работы;
   b. отказ работы системы < 6 ч из-за потери доступности системы безопасности;
   c. запрет аварийного отключения, вызвавший фатальные последствия для всей системы.
d) Критичность: экстремальная

Цель обеспечения безопасности: защита целостности и доступности участка 1 системы безопасности гидрокрекинга.
Политика безопасности: Коммуникации полевого уровня разрешены с Зоной Р1 (Участок 1, процесс гидрокрекинга). Чтение данных разрешено для зарегистрированных элементов системы в Зоне С1 (Участок 1, базовая система управления гидрокрекингом). Любые команды записи в зону извне запрещены. Все функции управления и программирования разрешены только внутри зоны.
Коммуникации между зонами: Пути к этой зоне могут быть проведены из зоны С1 и зоны Р1.
Стратегия обеспечения безопасности: все соединения с защищенной зоной должны быть проверены Контролирующей организацией.
Управление изменениями в процессе: любое изменение внутри зоны или пути должно быть согласованно с контролирующей организацией. Примеры: установка или замена оборудования, изменение политики безопасности, добавление исключений.

Управление системой безопасности

Перед запуском системы в боевом режиме необходимо провести тестирование, цель которого — про-

верка работоспособности АСУТП с установленными средствами безопасности.

Для этих целей у межсетевого Hirschmann Eagle Tofino предусмотрен тестовый режим. Это специальный режим, когда трафик в сети не блокируется межсетевым экраном, но при этом ведется протоколирование того, какой трафик будет заблокирован после включения файрвола. Тестовый режим позволяет отредактировать имеющиеся правила и удостовериться, что после включения рабочего режима файрвол не заблокирует необходимые для ТП данные.

Вместе с запуском системы в «боевом» режиме становится актуальным вопрос об управлении всеми средствами безопасности в централизованном режиме. Сети управления будут иметь множество путей передачи данных, распределенных по территории предприятия. В идеале, весь парк средств безопасности должен быть управляем из одного места. Например, для серии продуктов Eagle Tofino у Hirschmann существует программный пакет Tofino CMP (Central Management Platform), позволяющий контролировать параметры и работу всех аппаратных межсетевых экранов Eagle Tofino на предприятии.

Заключение

Последние компьютерные и сетевые технологии внесли серьезный вклад в повышение производительности и увеличение эффективности производства. Вместе с тем, как показал вирус Stuxnet, информационные технологии уязвимы перед новыми рисками в виде специального вредоносного ПО, направленного на промышленные системы и процессы. С распространением подобного рода угроз становится актуальным вопрос повышения уровня кибер-безопасности промышленных систем управления.

Стандарты ANSI/ISA-99 предлагают разделить сети передачи данных предприятия на зоны и пути и с помощью средств кибер-безопасности серьезно снизить риски заражения специализированным вредоносным ПО и вирусами-клонами Stuxnet промышленных объектов.

Список литературы

1. *Денисенко В.В.* Компьютерное управление технологическим процессом, экспериментом, оборудованием. М.: Горячая линия-Телеком. 2009.
2. *Шахновский Г.* Безопасность Систем SCADA и АСУТП.
3. *Eric Byres.* Using ANSI/ISA-99 standards to improve control system security. Industrial Ethernet Book. IEB Media GbR.

Лопухов Иван Владимирович *– специалист компании ПРОСОФТ.*
Контактный телефон (495) 234-06-36.
Http://www.prosoft.ru

«ДЕЛАЙТ 2000» использует технологии виртуализации для создания аудиовизуальных комплексов

Компания «ДЕЛАЙТ 2000» — ведущий российский системный интегратор в области комплексных аудиовизуальных решений для индустриальных и офисных объектов, а также для образовательных учреждений — заключила партнерское соглашение с компанией VMware, мировым лидером в области разработки ПО для виртуализации. Данное соглашение позволяет «ДЕЛАЙТ 2000» предлагать своим заказчикам инновационные AV-решения, опирающиеся на полную линейку продуктов VMware в области виртуализации серверов, сетей передачи данных, настольных компьютеров, приложений и информационных хранилищ. В настоящее время «ДЕЛАЙТ 2000» уже разрабатывает ряд решений с использованием продуктов VMware и ведущих вендоров профессионального AV-оборудования высшего класса. Примером может служить виртуальная рабочая среда для диспетчерских пунктов или сети переговорных комнат.

Сегодня AV-решения, в которых применяются технологии виртуализации, становятся все более востребованными как в офисной среде, так и в диспетчерских центрах. В первом случае повышается экономическая эффективность и управляемость AV-комплекса, а также возрастает мобильность сотрудников, которые получают возможность одинаково эффективно работать в офисе, дома и в дороге. В диспетчерском центре виртуализация высокопроизводительных профессиональных рабочих станций одновременно повышает надежность, гибкость и масштабируемость AV-решения, а также улучшает его экономические характеристики и увеличивает период времени до морального устаревания. По оценке компании «ДЕЛАЙТ 2000», рост популярности решений, объединяющих AV-технологии с элементами ИТ-инфраструктуры, отражает один из главных векторов развития современного профессионального AV-рынка.

Для «ДЕЛАЙТ 2000» выбор продуктовой линейки именно VMware оправдан еще и тем, что ее поддерживают многие ведущие производители AV-оборудования, являющиеся партнерами компании. Кроме того, технологии виртуализации можно использовать и на уровне отдельных решений, и как основу ИТ-инфраструктуры в целом. Это важно, поскольку все чаще в своих проектах «ДЕЛАЙТ 2000» создает комплексные решения «под ключ», отвечающие самым современным требованиям и включающие не только AV-инфраструктуру, но и инженерные, охранные и противопожарные системы, сети передачи данных, а также проработку архитектурно-строительных вопросов.

Http://www.d2k.ru www.delight2000.com