Эрик Байрс

# Использование стандартов ANSI/ISA-99 для обеспечения безопасности системы управления промышленным предприятием

**В настоящее время в промышленных системах управления наблюдаются две тенденции: постепенный переход средств управления на стандарт Ethernet и появление специфического промышленного вредоносного ПО, атакующего конкретные типы промышленных систем управления. Это две стороны одной медали. 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 стороны, вредоносное ПО нового типа теперь может вмешаться в производственный процесс и причинить крупный урон деятельности предприятия. О принципах противодействия существующим и потенциальным угрозам и защиты от них сети промышленного предприятия согласно стандартам ANSI/ISA-99 рассказывается в данной статье.**

## Введение. Как современные методы автоматизации отражаются на безопасности системы управления

В процессе слияния корпоративных сетей передачи данных с промышленными системами управления технологическими процессами возникла тенденция замены нестандартизированных сетей и сетей с собственными узкоспециализированными протоколами передачи данных доступным коммерческим оборудованием, использующим технологии Ethernet TCP/IP.

Эта тенденция в индустрии серьёзно повлияла на связанность процессов внутри систем управления в сторону их усложнения. Построение сетей АСУ ТП по принципу офисных сетей привело к миграции уязвимостей последних в промышленный IT-контур. 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 серьёзно возросло число сбоев и простоев оборудования из-за последствий вредоносного ПО и кибератак.

Интернет-ресурс www.securityincidents.org (RISI, The Repository for Industrial Security Incidents) – крупнейшая в мире база данных по инцидентам в сфере безопасности SCADA-систем и АСУ ТП. Анализ данного ресурса за период с 1982 по 2010 год показывает, что сбои в работе систем управления вызываются следующими факторами:

- 50% инцидентов произошло случайно;
- 30% было вызвано вредоносным ПО;
- 11% случаев произошло благодаря несанкционированному доступу извне;
- 9% инцидентов случилось из-за вредоносных действий изнутри.

Можно выделить *три источника проблем безопасности:*

*1. Уязвимости в программной части оборудования*

SCADA-системы и средства АСУ ТП, такие как ПЛК и распределённые системы управления, удалённые терминалы и интеллектуальные конечные устройства, проектировались из расчёта максимальной надёжности и возможности ввода/вывода в реальном времени. Проблемы защищённого 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 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 Интернет современные системы управления доступны из множества внешних ресурсов, с которых возможна потенциальная атака.

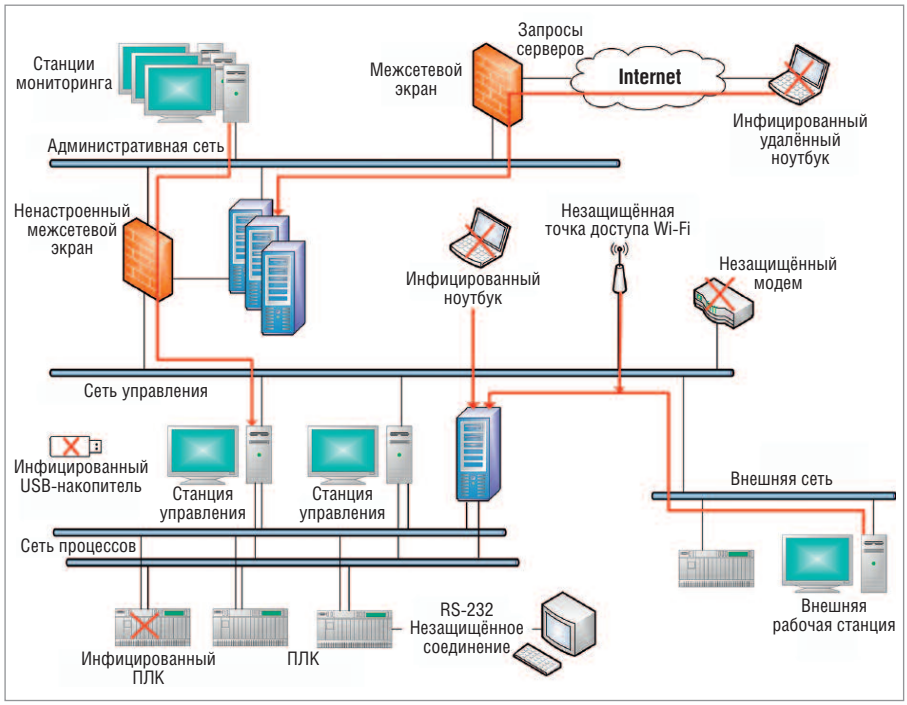


**Рис. 1. Возможные пути проникновения вредоносного ПО в систему управления**

К таким относятся интерфейсы удалённого управления и диагностики, серверы MES-систем, модемы удалённого доступа, последовательные соединения, беспроводные системы, мобильные станции оператора, USB-накопители, файлы данных о процессе, файлы документации (PDF). Перечисленные способы доступа к системам управления обычно не принимаются во внимание операторами и владельцами, они к тому же плохо задокументированы. На рис. 1 показаны возможные пути проникновения вредоносного ПО в систему. Стоит обратить особое внимание на то, что внешняя сеть Internet – только один путь из многих. Специалисты исследовательского центра NCCIC (National Cybersecurity and Communications Integration Center) в среднем насчитывают 11 способов доступа к закрытому контуру сети АСУ ТП, который, по сути, изолирован от общей сети предприятия. В отсутствие строгой политики разграничения сети производственного участка и общей сети прямых способов подключения к промышленному контуру может быть до 250. Последствия атаки вируса Stuxnet в 2010 году показали, что все открытые каналы доступа к промышленному сегменту сети могут быть задействованы вредоносным ПО.

*3. Недостаточная сегментация сети*

Сети передачи данных в АСУ ТП 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. Как результат, проблемы, возникшие на одном участке сети, быстро распространяются на всю сеть.

## Сегментирование сети и построение связей между сегментами по стандарту ANSI/ISA-99

Большинство компаний, решающих задачи 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. 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 удалённого управления, и все эти процессы несут потенциальную угрозу безопасности сети.

У инженеров АСУ ТП, работающих со 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 зависящих от производителей аппаратных средств автоматизации, например ПЛК. Отданная на откуп производителям компонентов автоматизации проблема безопасности фактически не решается. В конце 2011 года комитет US ICS-CERT (www.us-cert.gov) опубликовал исследование 137 продуктов для промышленной автоматизации со списками выявленных в их безопасности уязвимостей. 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 отчётов, опубликованных Американским национальным институтом стандартов (ANSI – American National Standards Institute). Комитет ISA-99, отвечающий за разработку стандартов, входит в Международную электротехническую 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, например, критичность для технологического процесса. Оборудование в каждой зоне имеет определённый 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 определённым каналам связи. Отслеживание и анализ трафика, проходящего по выделенным каналам, помогает предотвратить DoS-атаки (Denial of Service) и распространение вредоносного ПО, защитить соседние зоны, целостность и конфиденциальность трафика. В целом контроль каналов связи между зонами призван смягчить разницу между уровнями безопасности и требованиями к ней. Обеспечение контроля таких каналов – гораздо менее затратное мероприятие, чем модернизация каждого элемента внутри зоны до достижения соответствия заявленному уровню безопасности.

Важно понимать, что система стандартов ANSI/ISA-99 не определяет кон-

*Таблица 1*

**Ключевые требования к зонам и каналам 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 защищённую 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 отличающийся 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 неразрешённый трафик сети как внутрь, так и из защищённой зоны, содержащей критически важное оборудование. |

кретных методов или алгоритмов выделения зон и каналов внутри сети передачи данных предприятия. Взамен стандарты предлагают набор требований по обеспечению безопасности в зависимости от уровня рисков компании подвергнуться кибератакам. Риски заключаются не столько в возможности кибератаки, сколько в её последствиях, а уменьшение последствий достигается за счёт локализации их в выделенной зоне, максимально изолированной от остальных сегментов.

В таблице 1 приведён перечень основных разделов стандарта ANSI/ISA-99.02.01, относящихся к сегментации сети на зоны и к выделению каналов связи между ними.

## Выделение безопасных зон

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 разделяются по зонам, для которых устанавливается определённый уровень защиты.

К примеру, аппаратные средства на первом этапе могут быть разделены по производственным зонам, таким как складские средства автоматики, средства АСУ основного технологического процесса, средства финишной обработки продукции и т.п. Затем внутри этих областей возможна дальнейшая сегментация по функциональным уровням: MES-система, система операторского контроля (HMI), АСУ ТП (контроллеры ТП), система безопасности и т.д. Иногда выделяются зоны с оборудованием, реализующим определённый стандарт (МЭК 61850), или согласно рекомендациям производителя оборудования.

Каждая зона определяется набором атрибутов и характеристик. Вот некоторые рекомендуемые:

1. Характеристики зоны:
   - название зоны;
   - определение;
   - функциональная направленность.
2. Границы зоны.
3. Типовое оборудование (в идеале – перечень).
4. Изоляция от остальных зон.
5. Оценка рисков в пределах зоны:
   - возможности по обеспечению безопасности оборудования внутри зоны;
   - угрозы и уязвимости;
   - последствия возникновения «дыр» в системе безопасности;
   - возможный ущерб от кибератак.
6. Цели обеспечения безопасности.
7. Стратегии обеспечения безопасности.
8. Применение новых политик.
9. Обмен данными между зонами (требования к доступу).
10. 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, серьёзно отличаются от зоны, где используются Windows NT или ПЛК. Различия в возможностях и в уровнях потенциальных угроз порождают 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: Security for Industrial Automation and Control Systems: System Security Requirements and Security Assurance Levels («Безопасность для систем автоматизации и управления. Требования к безопасности систем и уровни обеспечения безопасности»).

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

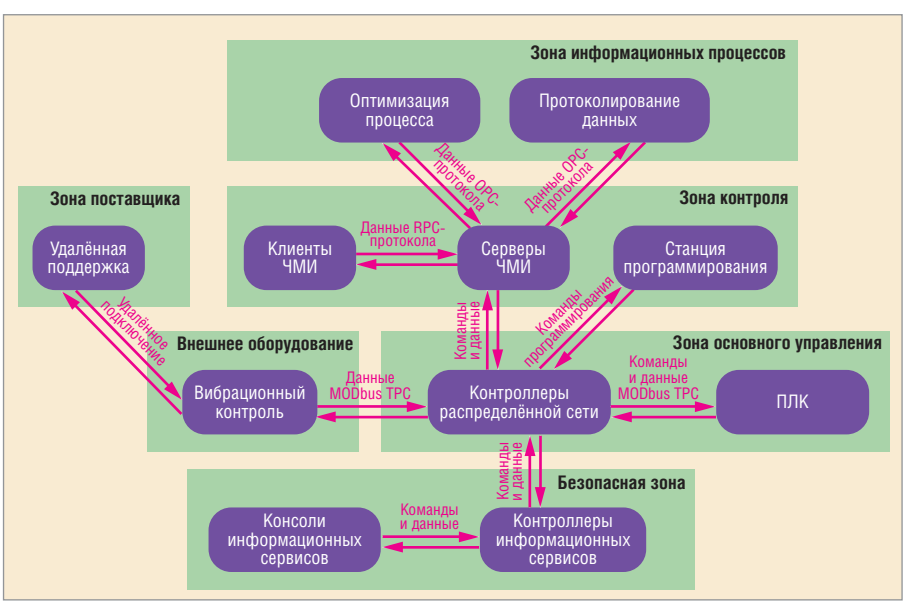


**Рис. 2. Пример диаграммы движения данных**

## Определение защищённых соединительных каналов между зонами

После сегментирования сети передачи данных на зоны следующим этапом является выделение связей между зонами, в терминологии стандарта – каналов. Каждый канал определён согласно зонам, которые он соединяет, техноло-

гиям, которые используются для связи между зонами, протоколам передачи данных и функциям безопасности в этих зонах. Трафик, проходящий по таким каналам, обычно детально известен. Утилиты-анализаторы трафика и протоколов дают достаточно полную информацию об обмене данными и о сервисах, использующих канал.

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

Диаграмма движения данных (рис. 2) – отличный инструмент для учёта данных в зонах и каналах между ними. Каждая зона может обозначаться прямоугольником, а движение определённых данных – вектором.

## Защита каналов связи

Как только каналы связи выделены и требования по обеспечению безопасности определены, настаёт время применять технологии по обеспечению безопасности. Две наиболее известные из них следующие:

- **межсетевые экраны** – это граничные устройства, контролирующие и инспектирующие трафик в зону и из неё. Они сравнивают проходящий через них трафик с заранее заложенными в них политиками безопасности, все пакеты данных, не относящиеся к разрешённому типу, удаляются. Обычно они конфигурируются на пропуск минимального объёма данных, достаточного для корректной работы всей системы. Особое внимание должно уделяться трафику с высоким уровнем риска, такому как команды программирования ПЛК или некорректно сформированные пакеты данных, которые могут использоваться для взлома системы. Отличия специальных промышленных межсетевых экранов здесь будут очевидны: они проектируются больше для инженеров АСУ ТП, чем для IT-специалистов, и в соответствии с потребностями в АСУ ТП в них заложены возможности глубокого анализа протоколов

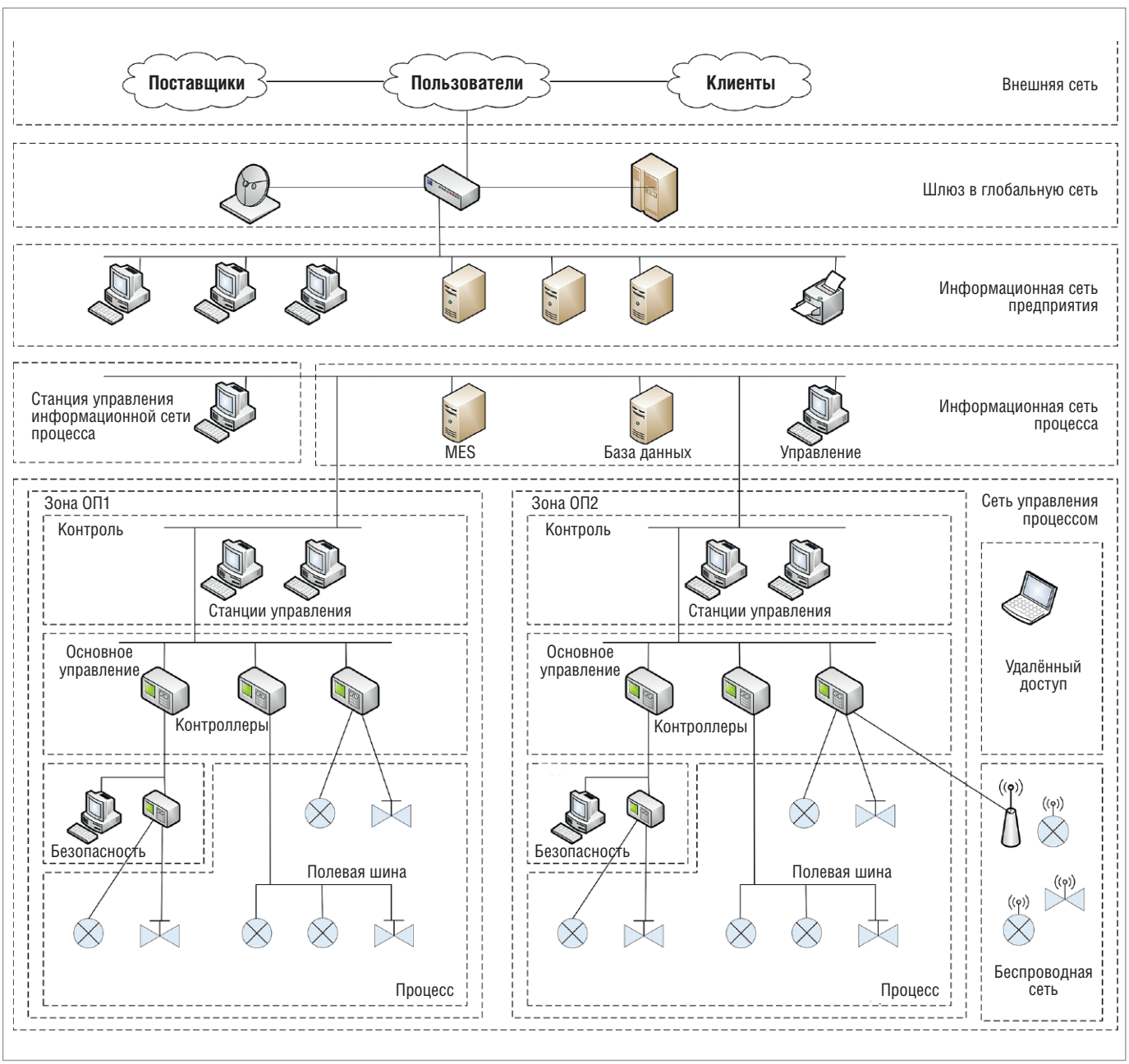


**Рис. 3. Схема ключевых операций нефтеперегонного завода**

SCADA-систем, таких как DNP3, Ethernet/IP, ModBus TCP;

- **сети VPN (виртуальные сети)** – это зашифрованные логические каналы связи, существующие поверх физической сети и реализующие приватную передачу данных и команд. Сессии 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 АСУ ТП и ИТ.

## Реальный пример сегментирования сети нефтеперегонного завода

Пример из нефтегазовой отрасли показывает процесс выделения зон и путей согласно стандарту ISA-99 в сети передачи данных предприятия с целью повышения безопасности и степени защищённости производственных процессов.

Большой нефтеперегонный завод выполняет несколько последовательных процессов, таких как дистилляция, гидроочистка, каталитический реформинг, заготовка и пр. Для упрощения схемы на рисунке 3 показаны только две производственные области, в реальности их, конечно, больше. Каждая область имеет свои базовые функции безопасности, контроля, системы ЧМИ и администрирования.

Эти системы объединены информационной сетью процесса (ИСП), в которой располагаются серверы MES-системы и баз данных процесса, доступных для общей сети предприятия и сети управления процессом. Дополнительно к процессу ОП 2 имеется доступ из беспроводной сети полевого уровня и через шлюз удалённого доступа для отладки инженерами АСУ ТП.

Разделение на зоны в данном случае производилось по функционалу, по уровням процессов, требованиям безопасности. Все функции управления принадлежат одной зоне управления процессом (зона А на рис. 4). 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 для процесса водоочистки.

Для каждой выделенной зоны необходимо составить список атрибутов, как описывалось ранее. Этот процесс интерактивный, на этапе описания зоны её границы могут быть изменены и выделены новые зоны. Пример написания атрибутов зоны S1 приведён во врезке.

В этом примере инженеры нефтеперегонного завода провели анализ системы на предмет выделения потенциальных источников угроз и 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.

### Пример написания атрибутов зоны S1

**Зона S1**

*Название:* Участок 1. Система безопасности гидрокрекинга.

*Определение зоны:* зона включает в себя все системы обеспечения безопасности гидрокрекинга.

*Контролирующая организация:* отдел АСУ ТП.

*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 серьёзными последствиями в случае взлома.

- **А.** 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.
- **Б.** Угрозы и уязвимости: уязвимости таких зон являются типовыми для существующих промышленных систем управления, использующих протокол Modbus для коммуникаций. Основные типы угроз:
  - DoS (Denial of Service) – атаки, направленные на вывод из строя системы коммуникаций;
  - внутренний или внешний несанкционированный доступ к рабочей станции;
  - считывание команд управления Modbus/TCP;
  - считывание ответов системы на посылку команд Modbus/TCP;
  - перепрограммирование функций безопасности.
- **В.** Последствия взлома системы безопасности:
  - отказ работы системы на 6 и более часов из-за ошибочного или аварийного завершения работы;
  - отказ работы системы менее чем на 6 часов из-за потери доступности системы безопасности;
  - запрет аварийного отключения, вызвавший фатальные последствия для всей системы.
- **Г.** 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 защищённой зоной должны быть проверены контролирующей организацией.

Управление изменениями в процессе: любое изменение внутри зоны или пути должно быть согласовано с контролирующей организацией. Примеры: установка или замена оборудования, изменение политики безопасности, добавление исключений. ■

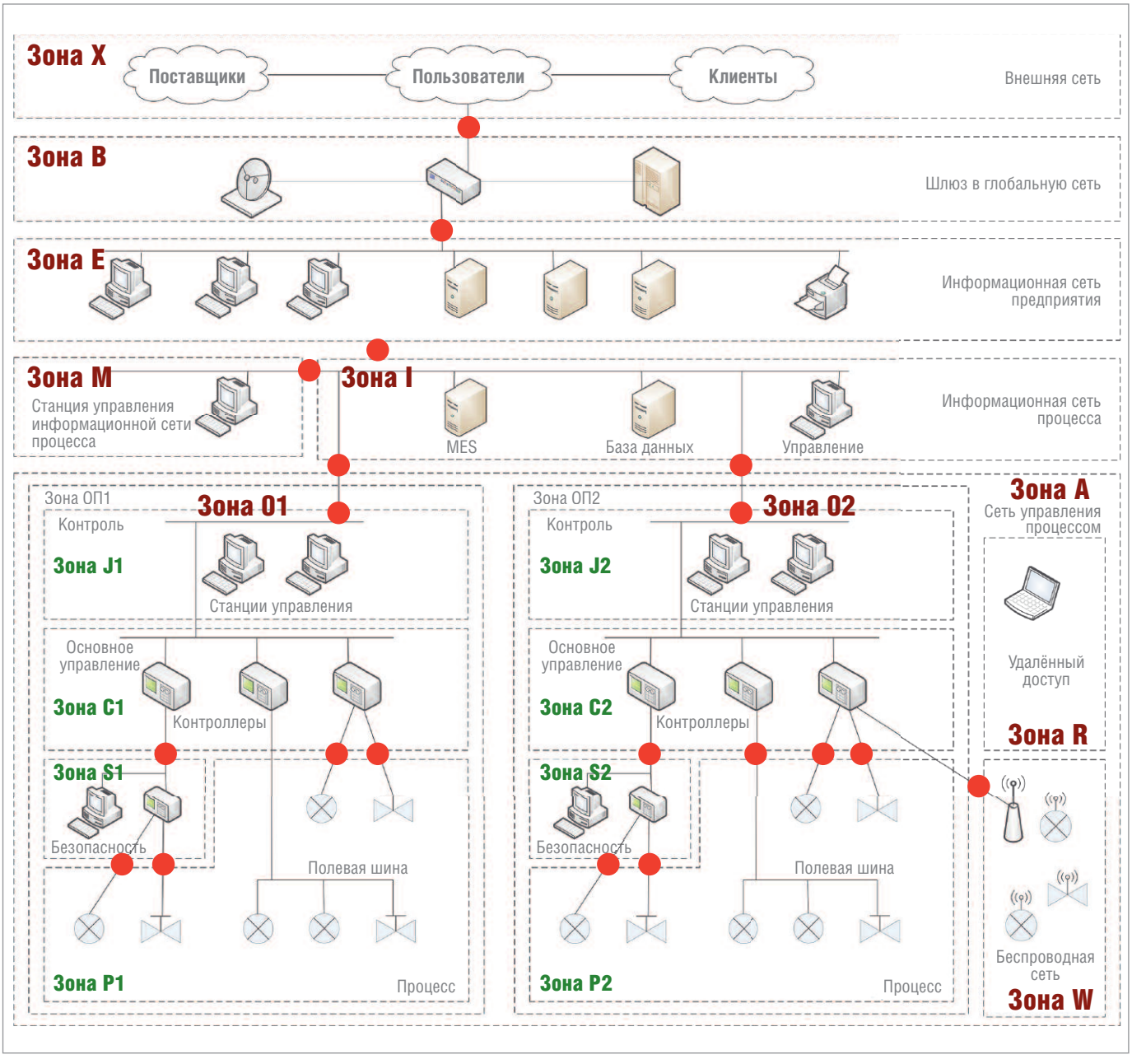


**Рис. 4. Схема зон и путей нефтеперегонного завода**

Имея определённые зоны, можно переходить к определению путей сообщения между ними. На рис. 4 они отмечены красными кругами. Термином «путь» здесь обозначены все информационные каналы между двумя зонами, это не только сетевые подключения, но и передача данных на съёмных носителях и пр.

## Реализация зон и путей 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. Пример – промышленный межсетевой экран Eagle Tofino компании Hirschmann (рис. 5).

Устройство Eagle Tofino изначально предназначено для интеграции в существующую сеть. Режим по умолчанию у межсетевого экрана – прозрачный. Таким образом, устройство интегрируется в сеть без каких-либо изменений в топологии или адресном пространстве. Затем оно может быть детально настроено для конкретных задач, на него могут устанавливаться программные компоненты, реализующие такие функции, как брандмауэр, VPN клиент/сервер, глубокий мониторинг конкретных протоколов передачи данных, например Modbus или OPC.

По стандарту ANSI/ISA-99 каждый путь, соединяющий зоны, должен содержать средство безопасности, каким является межсетевой экран. После оснащения всех путей сообщения межсетевыми экранами на последних можно активировать функцию брандмауэра для проверки всего трафика, проходящего через данный путь. Задачей брандмауэра будет блокировать любой вид трафика, заранее не разрешённый на данном пути.

## Тестирование и управление системой безопасности

Перед запуском системы в «боевом» режиме необходимо провести тестирование, цель которого – не столько проверка устойчивости сети к атакам, сколько проверка способности АСУ ТП работать корректно после внедрения средств безопасности.


**Рис. 5. Интегрированный модульный аппаратно-программный комплекс Hirschmann Eagle Tofino, предназначенный для создания безопасных зон внутри информационной сети предприятия**

Хороший способ проверить работоспособность – специальный режим тестирования, имеющийся у межсетевого экрана (режим «Тест» у Hirschmann Eagle Tofino). Это особый режим, в котором трафик в сети не блокируется межсетевым экраном, но при этом протоколируется, какой трафик будет заблокирован после включения брандмауэра. Тестовый режим позволяет отредактировать имеющиеся правила и удостовериться, что после включения рабочего режима брандмауэр не заблокирует необходимые для технологического процесса 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, распределённых по территории предприятия. В идеале весь парк средств безопасности должен быть управляемым из одного места. К примеру, 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

Передовые компьютерные и сетевые технологии внесли серьёзный вклад в повышение производительности и увеличение эффективности производства. Вместе с тем последствия атаки вируса Stuxnet в 2010 году дают основания говорить о том, что современные 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 кибербезопасности промышленных систем управления.

Стандарты ANSI/ISA-99 предлагают среду для компаний, желающих интегрировать функции безопасности в производственный процесс. Представленная в стандартах система разделения сети передачи данных предприятия на зоны и пути с помощью специальных промышленных межсетевых экранов и других средств кибербезопасности серьёзно снижает риски заражения специализированным вредоносным ПО и вирусами-клонами Stuxnet. ●

**Автор – технический директор и вице-президент группы Tofino Security компании Belden**

**Авторизованный перевод Ивана Лопухова, сотрудника фирмы ПРОСОФТ**
**Телефон: (495) 234-0636**
**E-mail: info@prosoft.ru**