На правах рукописи

Владимирский государственный
университет

04200911472 **Дерябин**

Александр Вячеславович

Защита информации в телекоммуникациях АСУ ТП химической промышленности

Специальность 05.12.13. - Системы, сети и устройства телекоммуникаций

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель: Доктор технических наук, профессор
Галкин А.П.

Владимир - 200

ОГЛАВЛЕНИЕ

г«.

ВВЕДЕНИЕ

Актуальность работы связана с широким использованием телекоммуникаций в автоматизированных системах управления технологическими процессами (АСУ ТП) и высоким уровнем опасности искажения или потери информации. Готовность организаций и предприятий, разрабатывающих и эксплуатирующих АСУ ТП, выполнять анализ их надёжности и безопасности является обязательным условием государственной и международной сертификации. Однако большинство систем управления технологическими процессами малой и средней сложности чаще всего проектируются малыми организациями в условиях жёстких финансовых и кадровых ограничений. И в силу этого вопросами информационной безопасности (ИБ) не занимаются вообще.

Если в атомной промышленности и энергетике последствия нарушения безопасности, в том числе информационной, могут быть масштабными и катастрофическими, то масштаб ущерба в АСУ ТП химической^ промышленности далеко не всегда так очевиден и велик. Размер ущерба и его характер определяется, прежде всего, самим технологическим процессом. При системном подходе необходимо рассматривать систему управления во взаимосвязи и взаимовлиянии не только с объектом управления (в данном случае - технологическим процессом), но и с источниками энергии, и с окружающей средой. В химической промышленности влияние на окружающую среду должно всегда подвергаться тщательному анализу не только в аварийном, но и в нормальном режиме работы АСУ ТП. Нарушение экологии может быть вызвано не только утечками и технологическими выбросами вредных веществ, но и, например, изменением температуры воды в водоёме при сбросе в него технологической воды, забранной из артезианской скважины для охлаждения процесса.

Обеспечить ИБ АСУ ТП на достаточно высоком уровне, при постоянно растущем уровне информатизации и постоянно

увеличивающемся количестве угроз, уже невозможно только комплексом внешних мер защиты. Автор

предлагает такой подход к обеспечению ИБ АСУ ТП, когда внешнюю защитную оболочку будет создавать комплексная система ИБ (включая системы мониторинга и управления информационной безопасностью, интегрированные с системами мониторинга и управления^ защищаемой системы), а внутренние барьеры образуют встроенные механизмы защиты программных и технических компонентов АСУ ТП. Такой подход можно назвать системным.

Обойти внешнюю защиту можно, внутреннюю — гораздо сложнее. Поэтому автор обращает особое внимание на преимущества разработки и применения программных и аппаратурных средств АСУ ТП, имеющих встроенные механизмы защиты, которыми пользователь может управлять для создания требуемой пропорции- механизмов- защиты в системе защиты информации (СЗИ).

Средства телекоммуникаций в АСУ ТП — это многообразие аппаратуры и программного обеспечения, которые должны иметь внутренние механизмы собственной безопасности. Поэтому от производителей технических средств и программного обеспечения АСУ ТП требуется разработка инструментов обеспечения безопасности своих продуктов.

Цель диссертационной работы - обоснование методов и разработка методик и алгоритмов обеспечения информационной безопасности и оценки информационной защищённости телекоммуникаций нижнего уровня АСУ ТП в химической промышленности.

Для достижения указанной цели в диссертации сформулированы, и решены следующие **научные и технические задачи:**

1. Исследованы типичные АСУТП в химической промышленности, ЗСАОА-системы, интеллектуальные датчики и телекоммуникации.

2. Выявлены угрозы ИБ, уязвимости СЗИ, особенности обеспечения ИБ АСУ ТП в химической промышленности.

3. Разработаны принципы выбора локальных сетей, БСАОА-систем, интеллектуальных датчиков и рекомендации по обеспечению ИБ оборудования и телекоммуникаций нижнего уровня АСУ ТП в химической промышленности.

4. Разработаны алгоритмы защиты от НСД в сетях нижнего уровня АСУ ТП. Экспериментальным исследованием доказана эффективность разработанных алгоритмов для повышения защищённости узлов сети.

5. Исследована эффективность использования физической скорости передачи в сетях нижнего уровня АСУ ТП при программных методах защиты.

6. Предложен метод аппаратурно-программной имитации для исследования СЗИ на базовом для исследуемой АСУ ТП программно-техническом комплексе (ПТК). Метод опробован при оценке СЗИ АСУ ТП «ПХВ-1», разработке и испытании рекомендаций по модернизации СЗИ.

7. Разработана методика оценки защищённости АСУ ТП. Обоснован показатель качества СЗИ АСУ ТП - уменьшение общего ущерба, наносимого воздействием угроз.

8. Разработана компьютерная программа для НСД в сеть МосИэиБ и*проведено экспериментальное исследование защищённости сети, датчиков и 8САОА-системы.

Методы исследования. В диссертации научные исследования основаны на методах математического моделирования, математической статистики, экспертных оценок при широком использовании программно- математического инструментария.

Основные теоретические результаты проверены в конкретных системах и с помощью моделирующих программ на компьютерах, а также в ходе испытаний и эксплуатации информационных сетей АСУ ТП.

Научная новизна диссертационной работы.

1. Проведён анализ и систематизация типичных структур АСУ ТП в химической промышленности, БСАОА-систем, интеллектуальных датчиков и телекоммуникаций. Выявлены угрозы ИБ, уязвимости СЗИ, особенности обеспечения ИБ АСУ ТП в химической промышленности.

2. Предложено создавать и использовать встроенные механизмы защиты оборудования и телекоммуникаций АСУ ТП в сочетании с комплексом внешних мер защиты. На основе такого системного подхода разработана методика создания СЗИ в АСУ ТП.

3. Разработаны алгоритмы защиты от НСД в сетях нижнего уровня АСУ ТП.

4. Проведён анализ и обоснован выбор показателя качества и методов оценки качества СЗИ в телекоммуникациях АСУ ТП. Разработана методика оценки качества СЗИ.

5. Проведены экспериментальные исследования разработанных методик и алгоритмов на действующих АСУ ТП.

Практическое значение диссертационной работы для разработчиков АСУ ТП и для эксплуатирующих предприятий заключается в облегчении задач выбора программных продуктов и технических средств с учётом ИБ, оценки информационной защищённости АСУ ТП с применением нормативной документации. Результаты работы полезны предприятиям, производящим аппаратуру и программное обеспечение для АСУ ТП.

Акты внедрения результатов диссертационной работы представлены в Приложении 9.

Диссертация состоит из введения, четырёх глав, заключения и приложений.

В первой главе выявлены угрозы информационной безопасности и уязвимости АСУ ТП. Проведен анализ типичных АСУ ТП в химической отрасли, ЗСАОА-систем и локальных сетей с точки зрения обеспечения безопасности.

Во второй главе рассмотрены особенности защиты информации в АСУ ТП химической промышленности, определены требования, к телеком-муникациям на всех уровнях иерархической структуры АСУ ТП. Выработаны рекомендации по выбору 8САГ>А-систем, аппаратуры и телекоммуникаций нижнего уровня АСУ ТП. Разработана методика создания систем защиты информации в АСУ ТП химической промышленности.

В третьей главе исследовано влияние программных мер защиты на эффективность использования физической скорости передачи в сетях МосИэиэ и РгоАЬш, при применении их на нижнем уровне АСУ ТП. С помощью разработанной автором программы проведена экспериментальная проверка защищённости телекоммуникаций нижнего уровня АСУ ТП от НСД. Разработаны алгоритмы доступа к узлам сети со стороны пульта и со стороны сети, отличающиеся оптимальным сочетанием методов защиты от НСД и обеспечивающие быстрое обнаружение вторжения. Сравнительное экспериментальное исследование нескольких устройств показало многократное (минимум в 5 раз) превосходство по защищённости узлов, в которых реализован разработанный автором алгоритм доступа. Проанализированы существующие механизмы защиты информации в АСУ ТП производства бумвинила «ПХВ-1» и выработаны рекомендации по модернизации СЗИ. Предложено применение программно-аппаратурных имитаторов на базе контроллеров ПТК для имитации нештатных ситуаций (сбоев, отказов, НСД), а также защитных мероприятий. Приведены результаты моделирования на имитаторах АСУ ТП «ПХВ-1» до и после введения дополнительных мер защиты информации.

В четвёртой главе исследована нормативная база российских и международных стандартов и руководств по информационной безопасности телекоммуникаций АСУ ТП. Обоснован показатель

качества, проведён обзор методов оценки качества СЗИ АСУ ТП. Разработана методика оценки защищённости АСУ ТП. Разработанная методика применена для оценки СЗИ АСУ ТП «ПХВ-1».

В приложениях приведены различные вспомогательные и справочные материалы, а также акты внедрения.

Основные положения диссертации опубликованы в следующих статьях:

1. Дерябин, А.В. Компоненты и технологии видеонаблюдения /А.В. Дерябин // Современные проблемы экономикии новые технологии исследований: сб. науч.тр., ч.2 / Филиал ВЗФЭИ в г. Владимире. - Владимир, 2006.-С.17-21.

2. Дерябин, А.В. Эффективность использования GSM канала в системах телекоммуникации АСУ ТП / А.В. Дерябин // Экономический журнал ВлГУ. - Владимир, 2006. - № 6. - С. 12-13.

3. Дерябин, А.В. Угрозы информационной безопасности и уязвимости АСУ ТП / А.В. Дерябин, В.М. Дерябин // Проектирование и технология электронных средств. - 2007. - № 1. - С. 47-51.

4. Дерябин, А.В. Методология создания систем защиты АСУ ТП / А.В. Дерябин // Известия института инженерной физики. - 2008. - № 4. - С. 11-14.

5. Дерябин, А.В. Обеспечение информационной безопасности ИС / А.В. Дерябин // Проектирование и технология электронных средств. — 2008. — № 3. - С. 7-10.

6. Дерябин, А.В. Интеллектуализация датчиков и информационная безопасность / А.В. Дерябин, В.М. Дерябин // Известия института инженерной физики. - 2009. -№ 2. - С. 7-12.

7. Дерябин, А.В. Применение алгоритма нечёткого вывода и нечёткой логики в защите информации / А.П. Галкин, А.В. Дерябин, Аль- Муриш Мохаммед, Е.Г. Суслова // Известия института инженерной физики. — 2009.-№2.-С. 13-15.

8. Дерябин, А.В. Комплексная или поэлементная защита? / А.В. Дерябин, В.М. Дерябин, Тахаан Осама // Перспективные технологии в средствах передачи информации - ПТСПИ-2009: материалы VIII международной научно- технической конференции. - Владимир: Изд-во ВлГУ, 2009. - С. 188.

1 УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УЯЗВИМОСТИ АСУ ТП

1.1 Телекоммуникации АСУ ТП

Автоматизированная система управления технологическим процессом (АСУ ТП) — комплекс программных и технических средств, предназначенный для автоматизации управления технологическим оборудованием на предприятиях. Под АСУ ТП обычно понимается комплексное решение, обеспечивающее автоматизацию основных технологических операций на производстве в целом или каком-то его участке, выпускающем относительно завершенный продукт.

В английской литературе для обозначения АСУ ТП обычно используется термины Process Control Systems или реже Automatic Control Systems (последнее определение, на взгляд автора, несколько абстрактно, так как не указывает на конкретное предназначение системы управления).

Здесь важно сделать акцент на слове «автоматизированная». Под этим подразумевается, что система управления отнюдь не полностью автономна (самостоятельна), и требуется участие человека (оператора) для реализации определенных задач. Выражение «пустил и забыл» для таких систем не подходит. Напротив, системы автоматического управления (САУ) предназначены для работы без какого-либо контроля со стороны человека и полностью автономны. Очень важно понимать эту принципиальную разницу между АСУ и САУ.

1.1.1 Типовая структура АСУ ТП

В большинстве современных автоматизированных систем управления технологическими процессами (АСУ ТП) можно выделить три уровня. На нижнем уровне располагаются аппаратные средства — датчики,

исполнительные механизмы, управляющие контроллеры. На среднем уровне находятся групповые контроллеры, устройства сопряжения с объектами. Верхний уро

вень реализуется на персональных компьютерах, где с помощью специальных пакетов (БСАБА систем) реализуется интерфейс с оператором- технологом, выполняющим супервизорное управление технологическим процессом.

Пример трёхуровневой системы управления сложным технологическим процессом показывает Рисунок 1.1. Количество контролируемых параметров в таких системах измеряется сотнями, управляемых параметров — десятками.

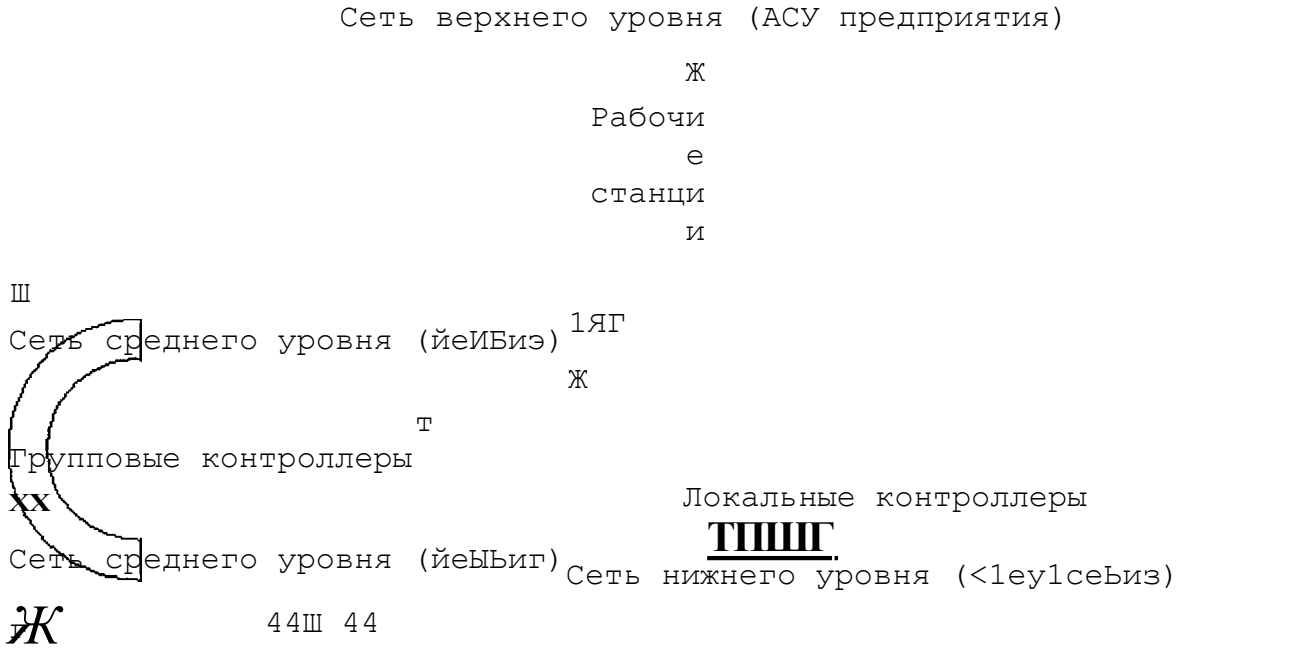


Рисунок 1.1- Типовая структура трёхуровневой АСУ ТП

Технологический процесс управляется с помощью исполнительных механизмов, а информация о параметрах технологического процесса снимается с помощью датчиков. Ввод информации о параметрах, вычисление управляющих воздействий и их выдача на исполнительные механизмы осуществляется локальными контроллерами ЛК или групповыми контроллерами ГК.

Координация управления процессом осуществляется рабочими (оператор-

скими) станциями РС с помощью локальной сети. Количество РС определяется в зависимости от сложности процесса, но их всегда больше одной, так

как применяется дублирование для повышения надежности. В свою очередь, РС объединены как между собой, так и с другими абонентами цеха (предприятия), с помощью локальной сети верхнего уровня типа Ethernet. Необходимо подбирать тип локальной сети и её параметры под конкретные требования: гарантированное время доставки; скорость передачи; объём пакетов; количество аппаратно реализованных функций в контроллерах сети и т.д.

Устройства сопряжения с объектом (УСО) преобразуют управляющие коды, выдаваемые процессором контроллера, в сигналы управления исполнительными механизмами (импульсные, дискретные, аналоговые), а сигналы датчиков преобразуют в коды для ввода в процессор. УСО располагаются внутри JIK или ГК. В последнее время имеется тенденция йнтеллектуализа-

ции датчиков, то есть размещение схем преобразования непосредственно в корпусе датчиков и передачи кодов в процессор по стандартному последовательному интерфейсу.

Датчики

1.1.2 Классификация АСУ ТП

В зарубежной литературе можно встретить довольно интересную классификацию АСУ ТП [1], в соответствие с которой все АСУ ТП делятся на три глобальных класса:

• SCADA (Supervisory Control and Data Acquisition). На русский язык этот термин можно перевести как «система телемеханики», «система телеметрии» или «система диспетчерского управления»». На взгляд автора, последнее определение точнее всего отражает сущность и предназначение системы - контроль и мониторинг объектов

с участием диспетчера. Тут необходимо некоторое пояснение. Термин SCADA часто используется в более узком смысле: так называют программный пакет визуализации технологического процесса. Однако в данном разделе под словом SCADA мы будем понимать целый класс систем управления.

- PLC (Programmable Logic Controller). На русский язык переводится как «программируемый логический контроллер» (или сокращенно ПЛК). Тут, как и в предыдущем случае, есть двусмысленность. Под термином ПЛК часто подразумевается аппаратный модуль для реализации алгоритмов автоматизированного управления. Тем не менее, термин ПЛК имеет и более общее значение и часто используется для обозначения целого класса систем.
- DCS (Distributed Control System). По-русски: распределенная система управления (РСУ). Тут никакой путаницы нет, все однозначно.

Справедливости ради надо отметить, что если в начале 90-х такая классификация не вызывала споров, то сейчас многие эксперты считают ее весьма условной. Это связано с тем, что в последние годы внедряются гибридные системы, которые по ряду характерных признаков можно отнести как к одному классу, так и к другому.

Автор предлагает не следовать делению АСУ ТП на SCADA, PLC и DCS, а рассматривать АСУ ТП в химической промышленности как распределенные системы, в состав которых входят PLC и SCADA.

1.2 Угрозы информационной безопасности АСУ ТП

Рассмотрим наиболее распространенные угрозы [2], которым подвержены современные АСУ ТП. В отличие от других автоматизированных информационных систем промышленные АСУ и АСУ ТП, особенно те, которые используются для управления критической инфраструктурой государства, имеют ряд особенностей, обусловленных их особым назначением, условиями эксплуатации, спецификой обрабатываемой в них информации и требованиями, предъявляемыми к

функционированию. Главной же особенностью этих систем является то, что с их помощью в автоматическом, либо автоматизированном режиме в реальном времени осуществляется управление физическими процессами и системами, от которых непосредственным образом зависит наша безопасность и жизнедеятельность: электричество, связь, транспорт, финансы, системы жизнеобеспечения, атомное и химическое производство и т.п. [3].

Поэтому обеспечение информационной безопасности таких систем является одной из важнейших задач разработчиков АСУ ТП.

Промышленные системы прошли путь от простейших программных и аппаратных средств до современных систем, в которых используются стандартные компьютеры и серверы, операционные системы семейства Microsoft Windows, стандартные SCADA-системы, сетевые протоколы TCP/IP, Web- браузеры, доступ в Интернет. Множество угроз в отношении этих систем значительно расширилось благодаря такой стандартизации, а также благодаря распространенной практике подключения промышленных систем к локальным сетям предприятия и использованию в них технологий беспроводного доступа [4].

1.2.1 Классификация угроз информационной безопасности АСУ ТП

Иметь представление о возможных угрозах, а также об уязвимых местах, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

Само понятие «угроза» в разных ситуациях зачастую трактуется по- разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать - вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в информационной безопасности, зависят от интересов субъектов информационных отношений, и от того, какой ущерб является для них неприемлемым.

Отметим, что некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных АСУ ТП [5]. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения АСУ ТП от качественного электропитания.

Угрозы можно классифицировать по разным критериям [6]:

1) по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;

2) по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

3) по способу осуществления (случайные, либо преднамеренные действия природного или техногенного характера);

4) по расположению источника угроз (внутри, либо вне рассматриваемой АСУ ТП);

5) по агенту угрозы (вредоносное ПО, пользователи и обслуживающий персонал АСУ ТП, хакеры, террористы).

В качестве основного мы будем рассматривать первый критерий (по V аспекту информационной безопасности), при необходимости привлекая остальные.

1.2.1.1 Наиболее распространенные угрозы доступности.

Самыми частыми и самыми опасными, с точки зрения размера ущерба, являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих промышленные системы.

Иногда такие ошибки и являются собственно угрозами: неправильно введенные данные или ошибка в программе, вызвавшая крах системы. Иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники - таковы обычно ошибки

администрирования. По некоторым данным, до 65 % потерь — следствие непреднамеренных ошибок.

Остальные угрозы доступности классифицируем по компонентам АСУ ТП, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой (чаще всего бывает при необходимости осваивать новые возможности системы и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Главными источниками внутренних отказов системы являются:

- случайное или умышленное отступление от правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- ошибки при конфигурировании и администрировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре можно рассматривать следующие угрозы:

- случайное или умышленное нарушение работы систем связи (телекоммуникации), электропитания, водо- или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание обслуживающего персонала или пользователей выполнять свои обязанности (беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые «обиженные» сотрудники — как нынешние, так и бывшие. Как правило, они стремятся нанести вред организа- ции-«обидчику», например:

- испортить оборудование;
- встроить логическую бомбу, которая со временем разрушит программы или данные;
- удалить данные.

Опасны, разумеется, стихийные бедствия, пожары, наводнения, землетрясения, ураганы. По статистике, на долю огня, воды и тому подобных факторов (среди которых самый опасный — перебой электропитания) приходится 13 % потерь, нанесенных промышленным системам.

1.2.1.2 Основные угрозы целостности.

На втором месте по размерам ущерба после непреднамеренных ошибок и упущений стоят кражи и подлоги. В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних.

С целью нарушения статической целостности злоумышленник, как правило, штатный сотрудник, может:

- ввести неверные данные;
- изменить данные.

Иногда изменяются содержательные данные, иногда - служебная информация.

Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и программы. Внедрение вредоносного ПО — пример подобного нарушения.

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

Так же к угрозам целостности можно отнести потерю информации при передаче по каналам связи [7]. Частичная потеря пакетов в сетях телекоммуникации АСУ ТП может привести к получению неверных результатов, или выполнению неверных управляющих воздействий.

1.2.1.3 Основные угрозы конфиденциальности.

Конфиденциальную информацию в АСУ ТП можно разделить на служебную и предметную. Служебная информация, такая как пароли пользователей, не относится к определенной предметной области, в информационной системе АСУ ТП она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно может привести к получению несанкционированного доступа ко всей информации, в том числе предметной.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе, а то и попросту теряет. И дело здесь не в

неорганизованности людей, а в изначальной непригодности парольной схемы. Невозможно помнить много разных паролей; рекомендации по их регулярной смене только усугубляют положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двум-трем легко запоминаемым и столь же легко угадываемым паролям.

Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена необходимая защита. Угроза же состоит в том, что кто-то случайно или специально может получить полный либо частичный доступ к системе. В этот класс попадает также передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным перехват данных. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), но идея одна - осуществить доступ к данным в тот момент, когда они наименее защищены.

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании системы, но и, что очень важно, при всех изменениях. Очень опасной угрозой являются выставки, на которые многие организации отправляют оборудование из производственной сети, со всеми хранящимися на них данными. Остаются прежними пароли, при удаленном доступе они продолжают передаваться в открытом виде. Это плохо даже в пределах защищенной сети организации, а в объединенной сети выставки — это может привести к самым плачевным последствиям.

Еще один пример изменения, о котором часто забывают, - это хранение данных на резервных носителях. Для защиты данных на основных носителях применяются развитые системы управления доступом; копии же нередко просто лежат в шкафах и получить доступ к ним могут многие.

Перехват данных — очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные

передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата [7, 8] хорошо проработаны, доступны, просты в эксплуатации, а установить их, например, на кабельную сеть может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных.

К угрозам, от которых очень трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь, например, системный администратор, способен прочитать практически любой файл, войти в систему с учетными данными любого

пользователя и т.д. Возможно также нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Таковы основные угрозы, которые наносят наибольший ущерб информационной системе АСУ ТП (Таблица 1.1) [13].

Таблица 1.1- Основные угрозы Способы нанесения ущерба	Объекты воздействий			
	Оборудование	Программы	Данные	Персонал
Раскрытие информации (конфиденциа льность)	Хищение носителей информации, подключение к линии связи, несанкциониро в анное использование ресурсов	Несанкционир о ванное копирование перехват	Хищение, копирование, перехват	Передача сведений о защите, разглашение, халатность

Потеря целостности информации (целостность)	Подключение, модификация, спец.вложения, изменение режимов работы, несанкционированное использование ресурсов	Внедрение «троянских коней» и «жучков»	Искажение, модификация	Вербовка персонала, «маскарад»
Нарушение работоспособности автоматизированной системы (доступность)	Изменение режимов функционирования, вывод из строя, хищение, разрушение	Искажение, удаление, подмена	Искажение, удаление, навязывание ложных данных	Уход, физическое устранение

1.3 Уязвимости промышленных систем

На начальном этапе развития в промышленных системах использовалось малоизвестное специализированное оборудование и программное обеспечение, а их сетевое взаимодействие с внешним миром было сильно ограничено. Круг возможных угроз был слишком узок, поэтому внимания вопросам информационной безопасности со стороны разработчиков и владельцев таких систем практически не уделялось. Со временем разработчики переходят на стандартные ИТ платформы и 8САГ)А-системы, а владельцы промышленных систем, с целью повышения эффективности управления, подключают их к смежным системам. Существующая тенденция к повышению открытости и стандартизации промышленных систем повышает их уязвимость к кибератa- кам, однако среди экспертов не существует единого мнения относительно того, насколько сложной для аутсайдера задачей является получение доступа к промышленной системе [3].

В промышленных системах критической инфраструктуры существуют те же самые уязвимости, что и в большинстве обычных ИТ систем. Кроме этого, особенности промышленных систем, обуславливают

существование в них уникальных уязвимостей, к которым можно отнести:

1. **Человеческий фактор.** Эксплуатацией промышленных и корпоратив-ных систем обычно занимаются разные подразделения. Персонал промышленных систем, как правило, достаточно далек от вопросов обеспечения информационной безопасности, в его составе нет соответствующих специалистов, а рекомендации ИТ персонала на него не распространяются. Основной задачей остается решение технологических проблем возникающих в ходе эксплуатации системы, обеспечение ее надежности и доступности, повышение эффективности и минимизация накладных расходов.

2. **Уязвимости операционных систем.** Уязвимости операционных систем свойственны и для промышленных и для корпоративных систем, однако установка программных коррекций в промышленных системах на регулярной основе зачастую не выполняется. Главной заботой администратора такой системы является ее бесперебойная работа. Установка предварительно не протестированных программных коррекций может повлечь серьезные неприятности, а на полноценное тестирование обычно нет ни времени, ни средств.

3. **Слабая аутентификация.** Использование общих паролей является обычной практикой для промышленных систем. Благодаря этому у персонала пропадает ощущение подотчетности за свои действия. Системы двухфактор- ной аутентификации используются довольно редко, а конфиденциальная информация зачастую передается по сети в открытом виде.

4. **Удаленный доступ.** Для управления промышленными системами до-вольно часто используется удаленный доступ по коммутируемым каналам или по VPN каналам через сеть Интернет. Это может приводить к серьезным проблемам с безопасностью.

5. **Внешние сетевые подключения.** Отсутствие соответствующей норма-тивной базы и соображения удобства использования порой приводят к

тому, что между промышленными и корпоративными системами создаются сетевые подключения. Существуют даже рекомендации по поводу использования «комбинированных» сетей, позволяющих упростить администрирование. Это может отрицательно сказаться на безопасности обеих систем.

6. **Средства защиты и мониторинга.** В отличие от корпоративных систем использование IDS, МЭ и антивирусов в промышленных системах не является распространенной практикой, а для анализа журналов аудита безопасности обычно не остается времени.

7. **Беспроводные сети.** В промышленных системах часто используются различные виды беспроводной связи, включая протоколы 802.11, как известно, не предоставляющие достаточных возможностей по защите [25].

8. **Удаленные процессоры.** Определенные классы удаленных процессоров, используемых в промышленных системах для контроля технологических процессов, содержат известные уязвимости. Производительность этих процессоров не всегда позволяет реализовать функции безопасности. Кроме того, после установки их стараются не трогать годами, на протяжении которых они остаются уязвимыми.

9. **Программное обеспечение.** Программное обеспечение промышленных систем обычно не содержит достаточного количества функций безопасности. Кроме того, оно не лишено архитектурных слабостей.

10. **Раскрытие информации.** Не редко владельцы промышленных систем сознательно публикуют информацию об их архитектуре. Консультанты и разработчики частенько делятся опытом и раскрывают информацию о бывших клиентах.

11. **Физическая- безопасность.** Удаленные процессоры и оборудование промышленных систем могут находиться за пределами контролируемой зоны. В таких условиях, они не могут физически контролироваться персоналом, и единственным механизмом физической

защиты становится использование железных замков и дверей, а такие меры уж точно не являются серьезным препятствием для злоумышленников.

Отсюда следует, что существует значительное количество уязвимостей, являющихся специфичными для промышленных систем. Эти уязвимости обуславливают особые требования' по безопасности и особые режимы эксплуатации таких систем [10].

1.4 Типичные АСУ ТП в химической промышленности и их телекоммуникации

АСУ ТП в химической промышленности имеют свои особенности, как в аппаратурной, так и в программной' составляющих. Для обеспечения информационной безопасности таких систем используются различные методы и средства на каждом из уровней реализации АСУ ТП. Для того чтобы выявить основные меры по защите информации, применяемые в АСУ ТП данной отрасли, был проведен анализ типичных АСУ ТП с точки зрения^ обеспечения безопасности. Были проанализированы восемь современных АСУ ТП различной степени сложности, внедренные на объектах химического производства и смежных отраслей.

Рассматриваются меры защиты информации в аппаратуре, в сетях нижнего уровня АСУ ТП, в сетях верхнего уровня АСУ ТП, а также в программ-

ных компонентах (БСАВА-системах).

Проанализированы 12 . наиболее распространенных БСАВА-систем, применяемых в химической промышленности (Таблица 1.2).

Таблица 1.2 - Наиболее распространенные SCADA-системы №	Название	Производитель	Страна произ-водитель	Веб-Сайт
1	SIMATIC WINCC	Siemens	Германия	www.sms-automation.ru www. automati on-dri ves.ru
2	TRACE MODE 6	Adastra Research Group	Россия	www.adastra.ru
3	GENESIS32	Iconics	США	www.iconics.com
4	INTOUCH	Wonderware	США	www.wonderware.ru
5	C1TECT	Citect	США	www.citect.com www.citect.ru
6	КРУГ-2000	НПФ «Круг»	Россия	www.krug2000.ru
7	RealFlex	RealFlex Technologies	Ирландия	www.realflex.ru
8	MasterSCADA	ЗАО «ИнСАТ»	Россия	www.insat.ru
9	ClearSCADA	Control Microsystems	Канада	www.controlmicrosystems.com www.plcsystems.ru
10	iFIX	GE FANUC	США, Япония	www.gefanuc.com/ru
11	1GSS	Seven Technologies	Дания	www.7t.dk www.soliton.com.ua
12	OpenSCADA	Нехависимые разработчики	Украина, разработчики из разных стран	diyaorg.dp.ua

Более подробные результаты анализа приведены в Приложении 1.

Основные механизмы безопасности в БСАИА-системах приведены в

Приложении 2, механизмы безопасности в системе ШТОИСН - в Приложении 3, справочная информация о 8САОА-системах приведена в Приложении 4. На основании проведенного анализа можно сделать следующие выводы.

Во всех проанализированных АСУ ТП в химической промышленности применяются следующие меры зашиты: в сетях АСУ ТП нижнего уровня - защита данных СЯС-кодом в протоколах нижнего уровня. Что касается аппаратуры, то наиболее используемыми мерами защиты являются - использование промышленных контроллеров, соответствующих требованиям пылебрыз- гозащищенности. В программном комплексе АСУ ТП и сетях верхнего уровня применяются: ведение архива событий, защита информации встроенными

средствами протокола Ethernet, самодиагностика программно-технических средств, защита от несанкционированного доступа с помощью пароля.

Во многих АСУ ТП применяются: дублирование сетей нижнего уровня. В аппаратуре — применение промышленных шкафов, соответствующих требованиям по пылебрызгозащите, применение искрозащищенных УСО, применение резервных источников питания, резервирование контроллеров и датчиков, применение высоконадежных промышленных сетевых устройств, применение энергонезависимых ОЗУ, а также применение звукового и светового оповещения об аварийных ситуациях. В программном комплексе и сетях верхнего уровня во многих АСУ ТП применяются: разграничение прав доступа и создание профилей пользователей, автодиагностика состояния сети, t расширенная экранная помощь оператору, блокирование определенных функций в случае аварии, коррекция системного времени, обеспечение «безударного» перехода в ручной режим и обратно, применение брандмауэров для разделения сетей, функции сторожевого таймера.

Редко в АСУ ТП в химической промышленности находят применение следующие меры защиты информации: создание сетей нижнего уровня на базе оптоволоконной технологии передачи данных. В аппаратуре — взрывобезо- пасные контроллеры и УСО, отапливаемые монтажные шкафы, отдельная программно-аппаратная система противоаварийной защиты. В программном комплексе АСУ ТП и сетях верхнего уровня редко применяются: резервирование сетей верхнего уровня, разбиение локальной сети на изолированные сегменты (подсети), создание сетей верхнего уровня на базе оптоволоконной технологии передачи данных, рекомендации оператору о действиях в аварийной ситуации, применение защищенного протокола Industrial Ethernet в сетях верхнего уровня.

Нет сведений о применении следующих мер защиты: в сетях нижнего уровня АСУ ТП: применение безопасного f-профиля протокола. В аппаратуре - применение «интеллектуальных датчиков». В программном комплексе - настройка разрешенного времени для входа пользователя, системы обнаружения несанкционированного доступа в систему.

На основе проведенного анализа были разработаны рекомендации по обеспечению информационной безопасности для проектировщиков АСУ ТП малой и средней сложности в химической промышленности. Эти рекомендации, безусловно, будут полезны и производителям программных продуктов и технических средств для АСУ ТП.

1.5 Основные проблемы информационной безопасности в химической промышленности

Практические проблемы информационной безопасности в химической промышленности обусловлены, прежде всего, спецификой производственных процессов и отрасли в целом. Особенностями АСУ ТП химического производства являются:

- Взрывоопасность химического производства.

• Необходимость обеспечения высокой надежности из-за экологической опасности.

• Среда, в которой находится аппаратура АСУ ТП, особенно нижнего уровня - агрессивная, поэтому, аппаратура должна быть стойкой к коррозии.

• Для обеспечения безопасности производственного процесса требуется разнесение объектов на большие расстояния (сотни метров), то есть, требуется создавать рассредоточенные АСУ ТП с локальными сетями большой протяженности, дублированными каналами связи. ■

• Многие датчики и исполнительные механизмы располагаются на открытом воздухе, следовательно, они должны работать в широком температурном диапазоне.

• Химические процессы обычно протекают медленно, поэтому не требуется высокого быстродействия АСУ ТП.

• Разработкой сложных АСУ ТП в химической промышленности занимаются крупные проектные организации с большим опытом работы, широкими финансовыми, кадровыми и техническими возможностями. Их проекты в наибольшей степени учитывают и вопросы обеспечения информационной безопасности.

• Проектированием АСУ ТП малой и средней сложности, как правило, занимаются малые проектные организации. Их проекты чаще всего вообще не учитывают проблемы информационной безопасности.

1.5.1 Телекоммуникации в АСУ ТП

1.5.1.1 Сети нижнего уровня АСУ ТП (полевые шины [11]).

Промышленные сети передачи данных — базовый элемент для построения АСУ ТП. Появление промышленных коммуникационных протоколов положило начало внедрению территориального распределенных систем управления, способных охватить множество технологических установок, объединить целые цеха, а иногда и

заводы. Сегодня известно более 30 стандартов коммуникационных сетей (Таблица 1.3 содержит сведения об основных промышленных протоколах и их технических характеристиках [12]), специально адаптированных для промышленного применения, и каждый год появляются новые прогрессивные технологии передачи данных. Коммуникационные сети в большей степени определяют качество, надежность и функциональность АСУ ТП в целом.

Проанализировав Таблицу 1.3 можно сделать следующие заключения:

- В АСУ ТП в химической промышленности чаще применяются протоколы Modbus (ASCII, RTU), Profibus (DP, PA) с одним ведущим. При наличии многих ведущих к каждому относится своя группа ведомых.
- Преобладает шинная топология сети.
- Максимальное расстояние передачи 1,2 км без ретрансляторов.
- Скорость.передачи в сети редко превышает 1 Мбит/с.
- В большинстве случаев в качестве линии связи применяется экранированная витая пара.
- Максимальное количество узлов в сети редко превышает 127.
- Обычно максимальная длина кадра 256 байт.
- Практически все протоколы имеют аппаратурную реализацию первых двух уровней модели OSI (физического и канального).

Сети передачи данных, входящие в состав АСУ ТП, можно условно разделить на два класса:

1. Полевые шины (Field Buses);
2. Сети верхнего уровня (операторского уровня, Terminal Buses).

В данной главе мы рассмотрим полевые шины, при этом сделаем акцент на методах обеспечения надежности и отказоустойчивости.

Главной функцией полевой шины является обеспечение сетевого взаимодействия между контроллерами и удаленной периферией (например, узлами ввода/вывода). К полевой шине могут также подключаться контрольно- измерительные приборы (Field Devices),

снабженные сетевыми интерфейсами. Такие устройства называют интеллектуальными (Intelligent Field Devices), так как они поддерживают высокоуровневые протоколы сетевого обмена.

Таблица 1.3- Технические характеристики основных протоколов полевых шин Протокол	Ведущий	Топология	Макс, расстояние передачи	Макс. Скорость передачи	Провод	Макс, количество станции	Макс. Длина кадра	Уровень 2	Стандарт
ASI	один	Шина, дерево	100м	167Кбит/с	2	32	4 бита	chip	EN50295
BITBUS	много	шина	300м/ 375Кбит/с	375Кбит/с	2	251	248байт	chip	IEEE1118
CAN	много	шина	500м/ 125Кбит/с 40м/1 Мбит/с	1 Мбит/с	2	64	8байт	chip	ISO 11898/ ISOl 1519
ControlNet	много	Шина, звезда, дерево	5км 250м/modes	5 Мбит/с	Коакс.	99	51Обайт	ASIC	Open specified
DeviceNet	много	шина	500м/ 125Кбит/с 100м/500Кбит/с	500Кбит/с	4	64	8байт	chip	Open specified
Foundation Fieldbus	много	шина	2000м, 9,5км всего	31,25Кбит/с	2	240	246байт	chip	Open specified
FIP	много	шина	2000м/1 Мбит/с	2,5Мбит/с	2	256	32байт	chip	EN50170
INTERBUS		кольцо	12,8км	500Кбит/с	2/8	255	64байт	chip	EN50253
LON	много	Шина, дерево	6,1км/ 5Кбит/с	1,2Мбит/с	2	2	228байт	chip	ANSI
Modbus Plus	много	шина	1,8км	1 Мбит/с	2	32	32байт	chip	proprietary
Profibus-Net	много	Шина, дерево	1,2км	76,8Кбит/с	2	32 ведущих, 125 ведомых	56байт	chip	EN50170
PROFYBUS FMS	много	шина	19,2км/ 9,6Кбит/с 200м/500Кбит/с	500Кбит/с	2	127	246байт	Chip/sw	EN50170
PROFYBUS DP	много	шина	1км/12Мбит/с (4повторителя)	12Мбит/с	2	127	246байт	ASIC	EN50170

PROFYBUS PA	один	шина	1,9км	93,75Кбит/с	2	32	246байт	ASIC	EN50170
SERCOS	один	кольцо	250м	16Мбит/с	2/ fiber	245	1ббайт	ASIC	IEC61491
Seriplex	один	шина	1 ОООфутов	250Кбит/с	4	510	32байт	ASIC	proprietary
SwiftNet	много	шина	360м	5Мбит/с	2	>1024	896байт	ASIC	proprietary

Пример полевой шины представлен на Рисунке 1.2.

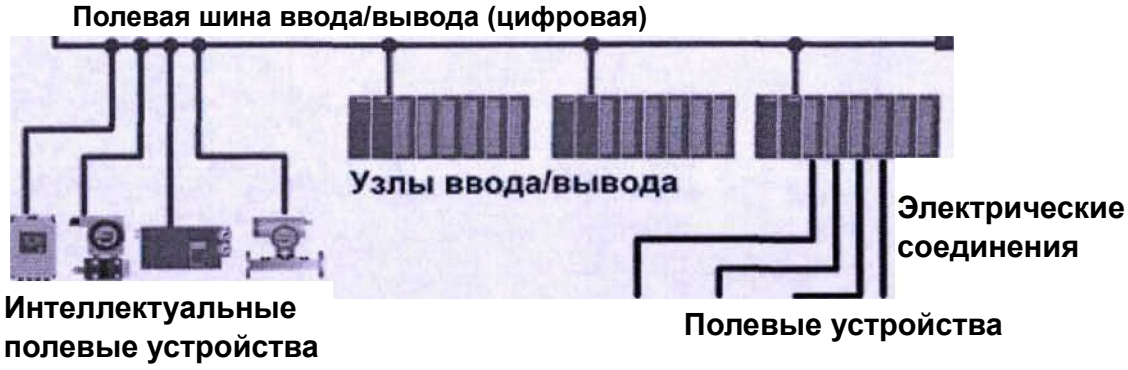


Рисунок 1.2 - Полевая шина

Как уже было отмечено, существует множество стандартов полевых шин, наиболее распространенные из которых приведены ниже:

1. Profibus DP
2. Profibus PA
3. Foundation Fieldbus
4. Modbus RTU
5. HART
6. DeviceNet

Несмотря на нюансы реализации каждого из стандартов (скорость передачи данных, формат кадра, физическая среда), у них есть одна общая черта - используемый алгоритм сетевого обмена данными, основанный на классическом принципе Master-Slave или его небольших модификациях.

Современные полевые шины удовлетворяют строгим техническим требованиям, **Контроллер** благодаря чему становится возможной их эксплуатация в тяжелых промышленных условиях. К этим требованиям относятся:

1. **Детерминированность.** Под этим подразумевается, что передача сообщения из одного узла сети в другой занимает строго фиксированный отрезок времени. Офисные сети, построенные по технологии Ethernet, - это отличный пример недетерминированной сети. Сам алгоритм доступа к разделяемой среде по методу CSMA/CD не определяет время, за которое кадр из одного узла сети будет передан другому, и, строго говоря, нет никаких гарантий, что кадр вообще дойдет до адресата. Для промышленных сетей это недопустимо. Время передачи сообщения должно быть ограничено и в общем случае, с учетом количества узлов, скорости передачи данных и длины сообщений, может быть заранее рассчитано.

2. **Поддержка больших расстояний.** Это существенное требование, ведь расстояние между объектами управления может порой достигать нескольких километров. Применяемый протокол должен быть ориентирован на использование в сетях большой протяженности.

3. **Защита от электромагнитных наводок.** Длинные линии в особенности подвержены пагубному влиянию электромагнитных помех, излучаемых различными электрическими агрегатами. Сильные помехи в линии могут исказить передаваемые данные до неузнаваемости. Для защиты от таких помех применяют специальные экранированные кабели, а также оптоволокно, которое, в силу световой природы информационного сигнала, вообще нечувствительно к электромагнитным наводкам. Кроме этого, в промышленных сетях должны использоваться специальные методы цифрового кодирования данных, препятствующие их искажению в процессе передачи или, по крайней мере, позволяющие эффективно детектировать искаженные данные принимающим узлом.

4. **Упрочненная механическая конструкция** кабелей и соединителей. Здесь тоже нет ничего удивительного, если представить, в каких условиях зачастую приходиться прокладывать коммуникационные линии. Кабели и соединители должны быть прочными, долговечными и приспособленными для использования в самых тяжелых окружающих условиях (в том числе агрессивных атмосферах).

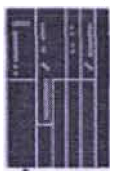
По типу физической среды полевые шины делятся на два типа:

1. Полевые шины, построенные на базе **оптоволоконного кабеля.** Преимущества использования оптоволокна очевидны: возможность построения протяженных коммуникационных линий (протяженностью до 10 км и-более); большая полоса пропускания; иммунитет к электромагнитным помехам; возможность прокладки во взрывоопасных зонах. Недостатки: относительно высокая стоимость кабеля; сложность физического подключения и соединения кабелей. Эти работы должны выполняться квалифицированными специалистами.

2. Полевые шины, построенные на базе **медного кабеля.** Как правило, это двухпроводной кабель типа «витая пара» со специальной изоляцией и экранированием. Преимущества: удобоваримая цена; легкость прокладки и выполнения физических соединений. Недостатки: подвержен влиянию электромагнитных наводок; ограниченная протяженность кабельных линий; меньшая по сравнению с оптоволокном полоса пропускания.

Итак, перейдем к рассмотрению методов обеспечения отказоустойчивости коммуникационных сетей, применяемых на полевом уровне. При проектировании и реализации этот аспект становиться ключевым, так как в большой степени определяет характеристики надежности всей системы управления в целом.

На Рисунке 1.3 изображена базовая архитектура полевой шины - одиночная (нерезервированная). Шина связывает контроллер С1 и четыре узла ввода/вывода 101-Ю4. Очевидно, что такая архитектура наименее отказоустойчива, так как обрыв шины, в зависимости от его локализации, ведет к потере коммуникации с одним, несколькими или всеми узлами шины.



Контроллер
С1

Шина ввода/вывода
----------С----------1----------1—----------г----------"

¡1]]]]] 1ЕШ *ШШ* В11

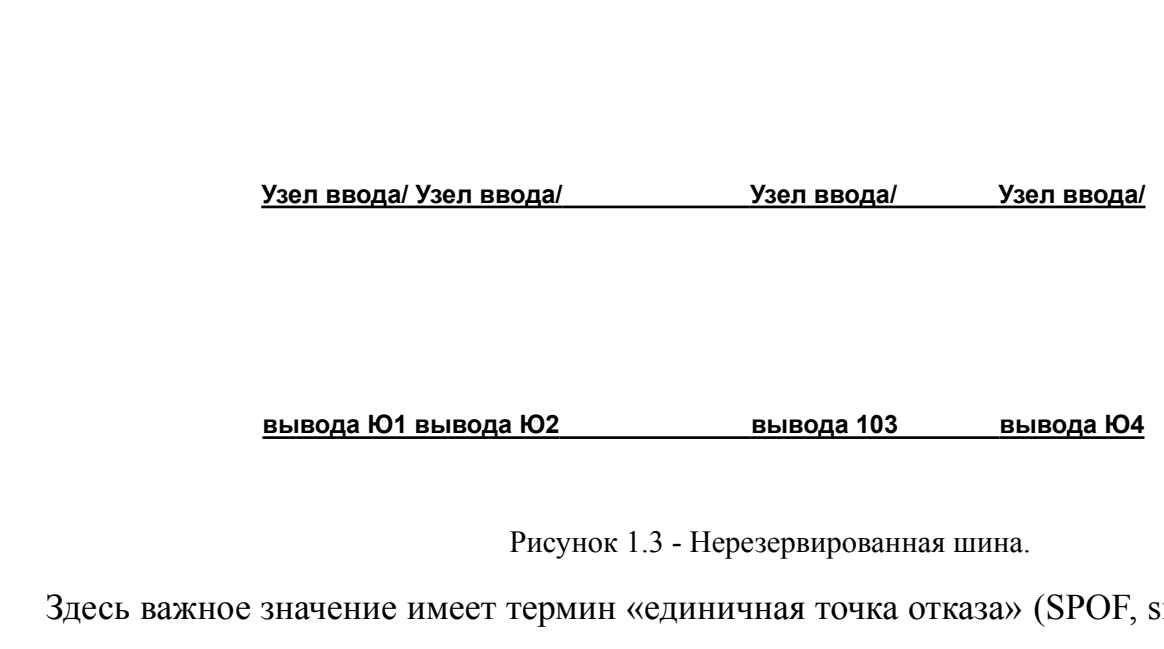


Рисунок 1.3 - Нерезервированная шина.

Здесь важное значение имеет термин «единичная точка отказа» (SPOF, single point of failure). Под этим понимается место в системе, отказ компонента или обрыв связи в котором приводит к нарушению работы всей системы.

На Рисунке 1.4 показана конфигурация в виде дублированной полевой шины, связывающей резервированный контроллер с узлами ввода/вывода. Каждый узел ввода/вывода снабжен двумя интерфейсными модулями. Если не считать сами модули ввода/вывода, которые резервируются редко, в данной конфигурации единичной точки отказа нет.

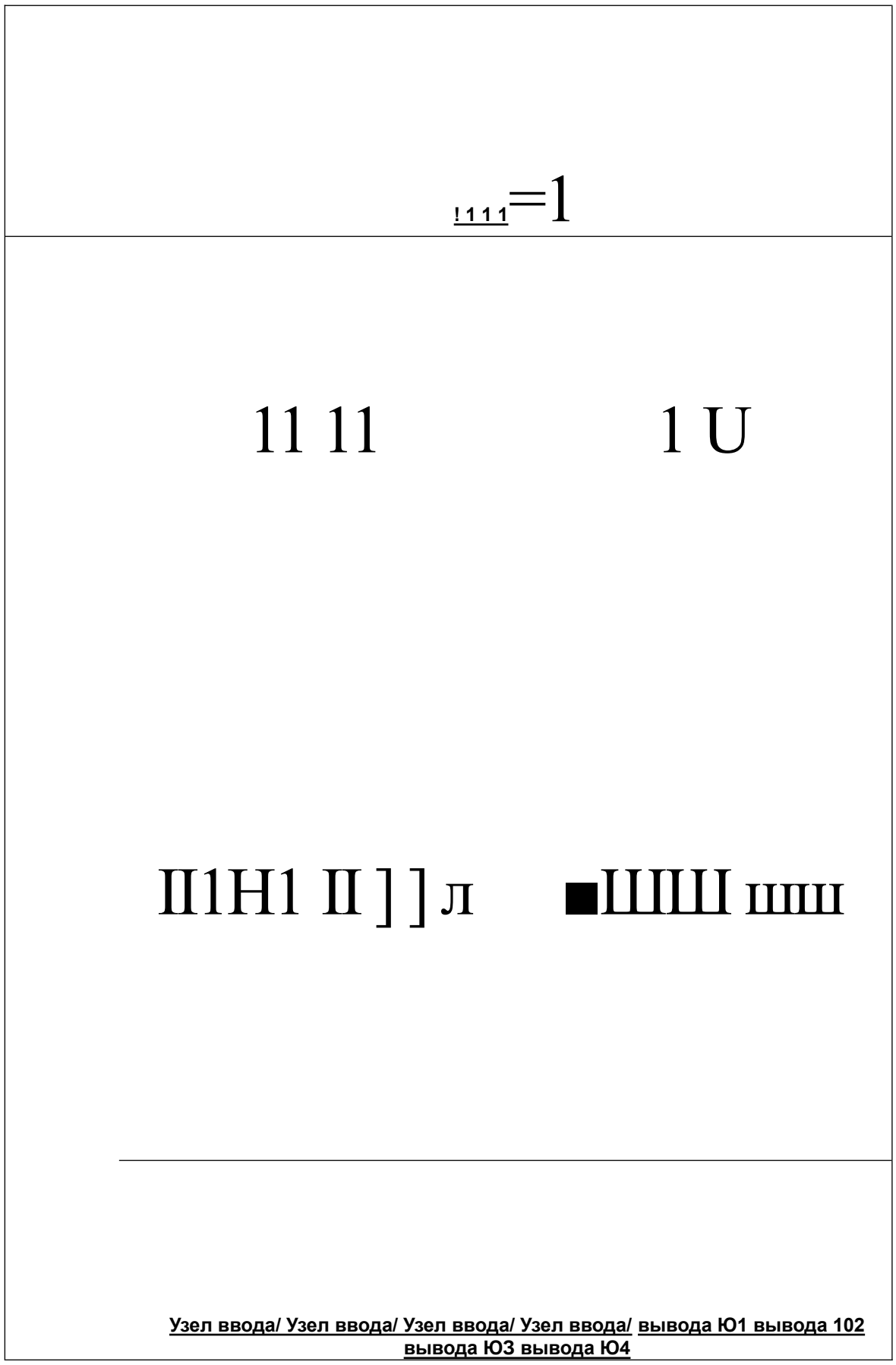

=1
11 11
1 U
II1H1 II]] л
■ШШШ шшш
Узел ввода/ Узел ввода/ Узел ввода/ Узел ввода/ вывода Ю1 вывода 102 вывода ЮЗ вывода Ю4

Рисунок 1.4 - Резервированная шипа.

Вообще, при построении отказоустойчивых АСУ ТП стараются, чтобы единичный отказ в любом компоненте (линии связи) не влиял на работу всей системы. В этом плане конфигурация в виде дублированной полевой шины является наиболее распространенным техническим решением.

На Рисунке 1.5 показана конфигурация в виде оптоволоконного кольца. Контроллер и узлы ввода/вывода подключены к кольцу с помощью резервированных медных сегментов. Для состыковки медных сегментов сети с опто-

волоконными применяются специальные конверторы среды передачи данных «медь<—>оптоволокно» (OLM, Optical Link Module). Для каждого из стандартных протоколов можно выбрать соответствующий OLM.

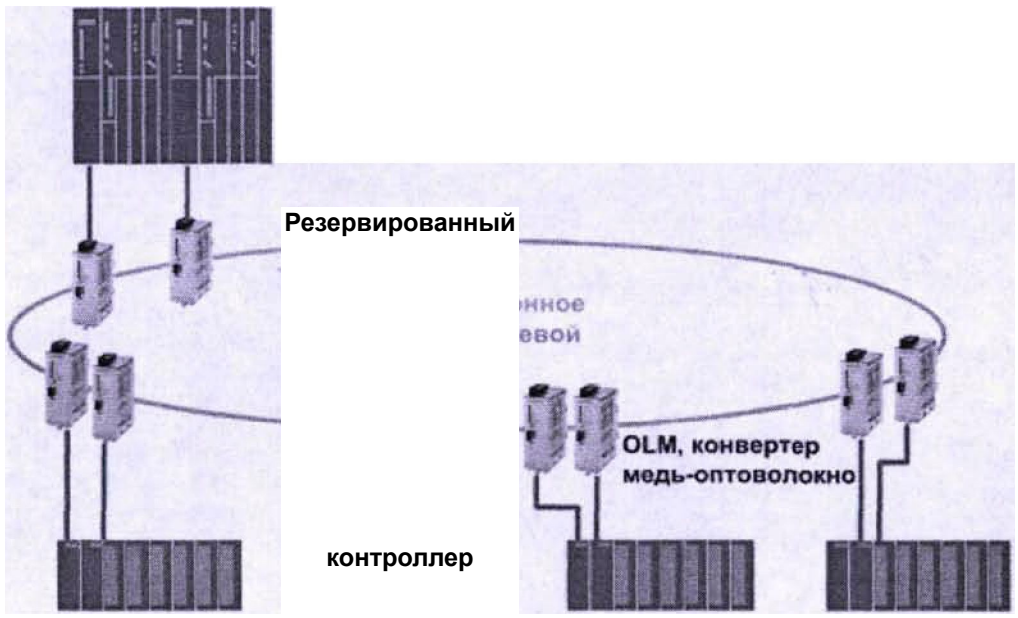


Рисунок 1.5 - Одинарное оптоволоконное кольцо.

Как и дублированная шина, оптоволоконное кольцо устойчиво к возникновению одного обрыва в любом его месте. Система такой обрыв вообще не заметит, и переключение на резервные интерфейсные и коммуникационные модули не произойдет. Более того, обрыв одного из двух медных сегментов,

соединяющих узел с оптоволоконным кольцом, не приведет к потере связи с этим узлом. Однако второй обрыв кольца может привести к неработоспособности системы. В общем случае два обрыва кольца в диаметрально

противоположных точках ведут к потере коммуникации с половиной подключенных узлов.

На Рисунке 1.6 изображена конфигурация с двойным оптическим кольцом. В случае если в результате образования двух точек обрыва первичное кольцо выходит из строя, система переключается на вторичное кольцо. Очевидно, что такая архитектура сети является наиболее отказоустойчивой. На Рисунке 1.6 пошагово изображен процесс деградации сети. Обратите внимание, сколько отказов система может перенести до того, как выйдет из строя.

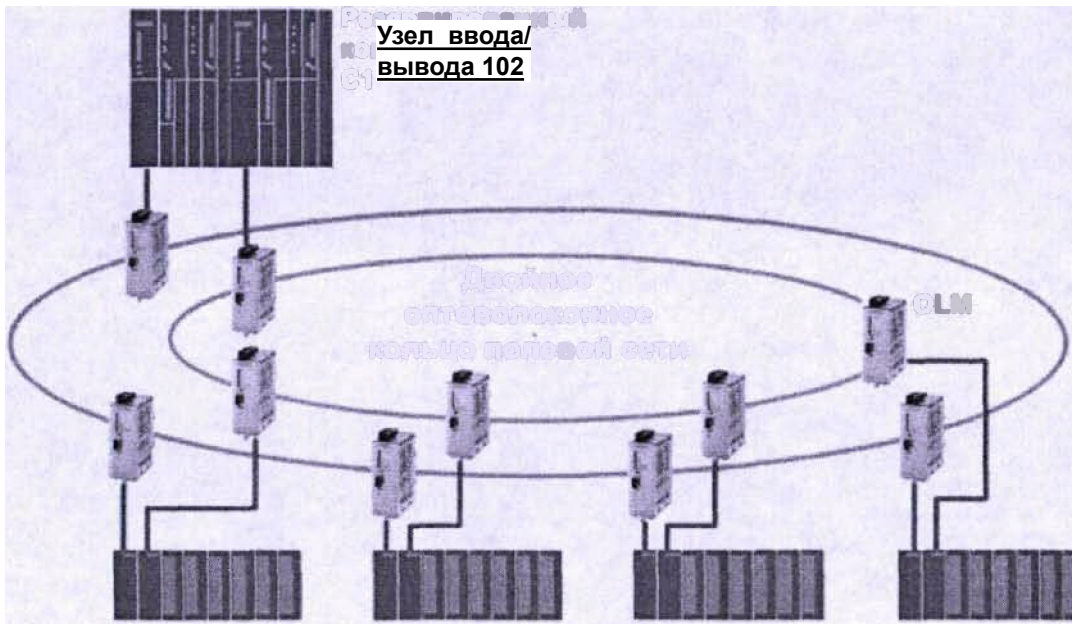
Резервированный

контроллер

С1

01.M

Двойное оптоволоконное кольцо полевой сети



Медный участок сети **Оптоволоконный участок сети**

Рисунок 1.6 - Резервированное оптоволоконное кольцо.

1.5.1.2 Промышленные сети верхнего уровня АСУ ТП.

Сети верхнего уровня служат для передачи данных между контроллерами, серверами и операторскими рабочими станциями [13]. Иногда в состав таких сетей входят дополнительные узлы: центральный сервер архива, сервер промышленных приложений, инженерная станция и т.д. Но это уже опции.

В отличие от стандартов полевых шин, на верхнем уровне большого разнообразия типов сетей нет. Фактически, большинство сетей верхнего

уровня, применяемых в современных АСУ ТП, базируется на стандарте Ethernet (IEEE 802.3) или на его более быстрых вариантах Fast Ethernet и Gigabit Ethernet. При этом, как правило, используется полный стек коммуникационных протоколов TCP/IP. В этом плане сети операторского уровня очень похожи на обычные ЛВС, применяемые в офисных приложениях. Широкое промышленное применение сетей Ethernet обусловлено следующими очевидными моментами:

1. Промышленные сети верхнего уровня объединяют множество операторских станций и серверов, которые в большинстве случаев представляют собой персональные компьютеры. Стандарт Ethernet отлично подходит для организации подобных ЛВС; для этого необходимо снабдить каждый компьютер лишь сетевым адаптером. Коммуникационные модули Ethernet для промышленных контроллеров просты в изготовлении и легки в конфигурировании. Стоит отметить, что многие современные контроллеры, уже $_4$имеют встроенные интерфейсы для подключения к сетям Ethernet.

2. На рынке существует большой выбор недорого коммуникационного оборудования для сетей Ethernet, в том числе специально адаптированного для промышленного применения.

3. Сети Ethernet обладают большой скоростью передачи данных. Например, стандарт Gigabit Ethernet позволяет передавать данные со скоростью до 1 Gb в секунду при использовании витой пары категории 5. Как будет понятно дальше, большая пропускная способность сети становится чрезвычайно важным моментом для промышленных приложений.

4. Очень частым требованием является возможность состыковки сети АСУ ТП с локальной сетью завода (или предприятия). Как правило, существующая ЛВС завода базируется на стандарте Ethernet. Использование единого сетевого стандарта позволяет упростить интеграцию АСУ ТП в общую сеть предприятия, что становится особенно

ощутимым при реализации и развертывании систем верхнего уровня типа MES.

Однако у промышленных сетей верхнего уровня есть своя специфика, обусловленная условиями промышленного применения. Типичными требованиями, предъявляемыми к таким сетям, являются:

1. Большая пропускная способность и скорость передачи данных. Объем трафика напрямую зависит от многих факторов: количества архивируемых и визуализируемых технологических параметров, количества серверов и операторских станций, используемых прикладных приложений и т.д. В отличие от полевых сетей жесткого требования детерминированности здесь нет: строго говоря, неважно, сколько времени займет передача сообщения от одного узла к другому - 100 мс или 700 мс (естественно, это не важно, пока находится в разумных пределах). Главное, чтобы сеть в целом могла справляться с общим объемом трафика за определенное время. Наиболее интенсивный трафик идет по участкам сети, соединяющим серверы и операторские станции (клиенты). Это связано с тем, что на операторской станции технологическая информация обновляется в среднем раз в секунду, причем передаваемых технологических параметров может быть несколько тысяч. Но и тут нет жестких временных ограничений: оператор не заметит, если информация будет обновляться, скажем, каждые полторы секунды вместо положенной одной. Если контроллер (с циклом сканирования в 100 мс) столкнется с 500-милисекундной задержкой поступления новых данных от датчика, это может привести к некорректной отработке алгоритмов управления.

2. Отказоустойчивость. Достигается, как правило, путем резервирования коммуникационного оборудования и линий связи по схеме так, что в случае выхода из строя коммутатора или обрыва канала, система управления способна в кратчайшие сроки (не более 1-3 с) локализовать место отказа, выполнить автоматическую перестройку

топологии и перенаправить трафик на резервные маршруты. Далее мы более подробно остановимся на схемах обеспечения резервирования.

3. Соответствие сетевого оборудования промышленным условиям эксплуатации. Под этим подразумеваются такие немаловажные технические меры, как: защита сетевого оборудования от пыли и влаги; расширенный температурный диапазон эксплуатации; увеличенный цикл жизни; возможность удобного монтажа на DIN-рейку; низковольтное питание с возможностью резервирования; прочные и износостойкие разъемы и коннекторы. По функционалу промышленное сетевое оборудование практически не отличается от офисных аналогов, однако, ввиду специального исполнения, стоит дороже.

Говоря о промышленных сетях, построенных на базе технологии Ethernet, часто используют термин Industrial Ethernet, намекая тем самым на их промышленное предназначение. Сейчас ведутся обширные дискуссии о выделении Industrial Ethernet в отдельный промышленный стандарт, однако на данный момент Industrial Ethernet — это лишь перечень технических рекомендации по организации сетей в производственных условиях, и я является, строго говоря, неформализованным дополнением к спецификации физического уровня стандарта Ethernet.

Есть и другая точка зрения на то, что такое Industrial Ethernet. Дело втом, что в последнее время разработано множество коммуникационных протоколов, базирующихся на стандарте Ethernet и оптимизированных для передачи критичных ко времени данных. Такие протоколы условно называют протоколами реального времени, имея в виду, что с их помощью можно организовать обмен данными между распределенными приложениями, которые критичны ко времени выполнения и требуют четкой временной синхронизации. Конечная цель - добиться относительной детерминированности при передаче данных. В качестве примера Industrial Ethernet можно привести:

1. Profinet;
2. EtherCAT;
3. Ethernet Powerlink;
4. Ether/IP.

Эти протоколы в различной степени модифицируют стандартный стек TCP/IP, добавляя в него новые алгоритмы сетевого обмена, диагностические функции, методы самокорректировки и функции синхронизации, оставляя

при этом канальный и физический уровни Ethernet неизменными. Это позволяет использовать новые протоколы передачи данных в существующих сетях Ethernet с использованием стандартного коммуникационного оборудования.

Теперь рассмотрим конкретные конфигурации сетей операторского уровня. На Рисунке 1.7 показана самая простая — базовая конфигурация. Отказ любого коммутатора или обрыв канала связи ведет к нарушению целостности всей системы.

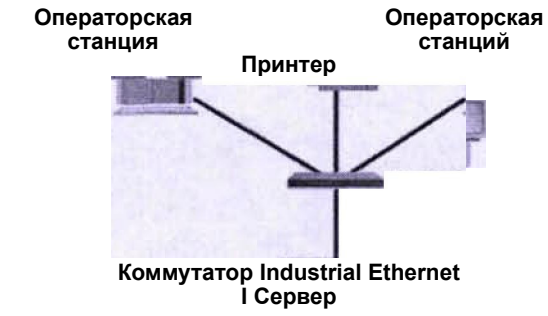
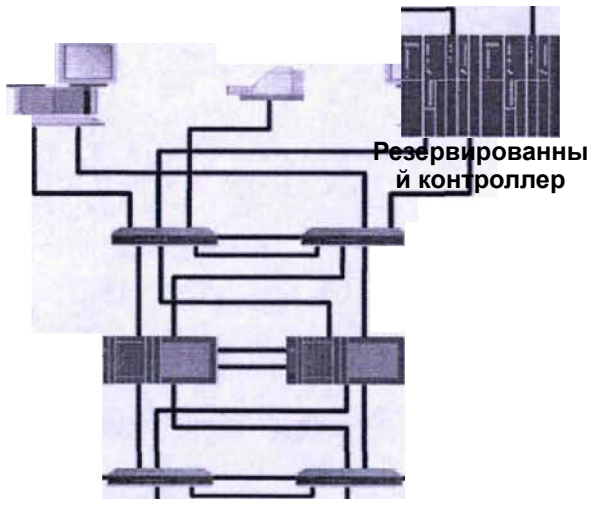


Рисунок 1.7 - Нерезервированная конфигурация сети верхнего уровня.

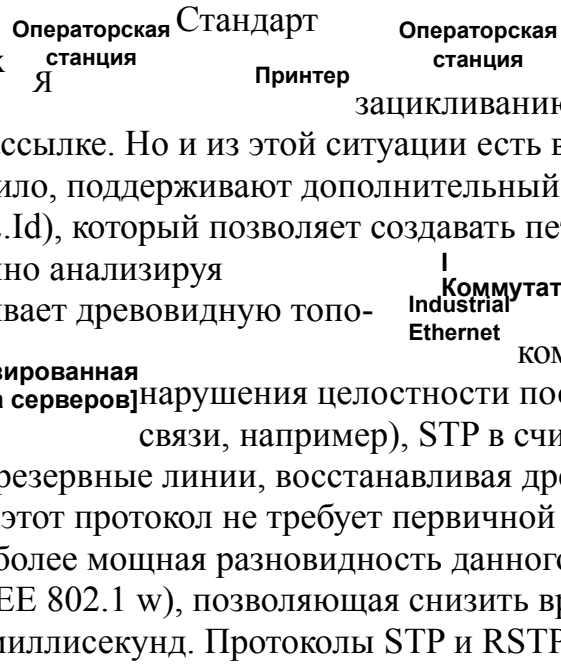
Такая простая конфигурация подходит лишь для систем управления, внедряемых на некритичных участках производства (водоподготовка для каких-нибудь водяных контуров или, например, приемка молока на молочном заводе). Для более ответственных технологических участков такое решение явно неудовлетворительно.

На Рисунке 1.8 показана отказоустойчивая конфигурация с полным резервированием. Каждый канал связи и сетевой компонент резервируется. Обратите внимание, сколько отказов переносит система прежде, чем теряется коммуникация с одной рабочей станцией оператора. Но даже это не выводит систему из строя, так как остается в действии вторая, страхующая рабочая станция.

Рисунок 1.8 - Полностью резервированная конфигурация сети верхнего уровня.



Резервирование неизбежно ведет к возникновению петлевидных участков сети - замкнутых маршрутов. Стандарт Ethernet, строго говоря, не допускает петлевидных топологий, так как это может привести к зацикливанию пакетов особенно при широковещательной рассылке. Но и из этой ситуации есть выход. Современные коммутаторы, как правило, поддерживают дополнительный прокол Spanning Tree Protocol (STP, IEEE 802.Id), который позволяет создавать петлевидные маршруты в сетях Ethernet, Постоянно анализируя конфигурацию сети, STP автоматически выстраивает древовидную топологию, переводя избыточные коммуникационные линии в резерв. В случае нарушения целостности построенной таким образом сети (обрыв связи, например), STP в считанные секунды включает в работу необходимые резервные линии, восстанавливая древовидную структуры сети. Примечательно то, что этот протокол не требует первичной настройки и работает автоматически. Есть и более мощная разновидность данного протокола Rapid Spanning Tree Protocol (RSTP, IEEE 802.1 w), позволяющая снизить время перестройки сети вплоть до нескольких миллисекунд. Протоколы STP и RSTP позволяют



создавать произвольное количество избыточных линий связи и являются обязательным функционалом для промышленных коммутаторов, применяемых в резервированных сетях.

На Рисунке 1.9 изображена резервированная конфигурация сети верхнего уровня, содержащая оптоволоконное кольцо для организации связи между контроллерами и серверами. Иногда это кольцо дублируется, что придает системе дополнительную отказоустойчивость.

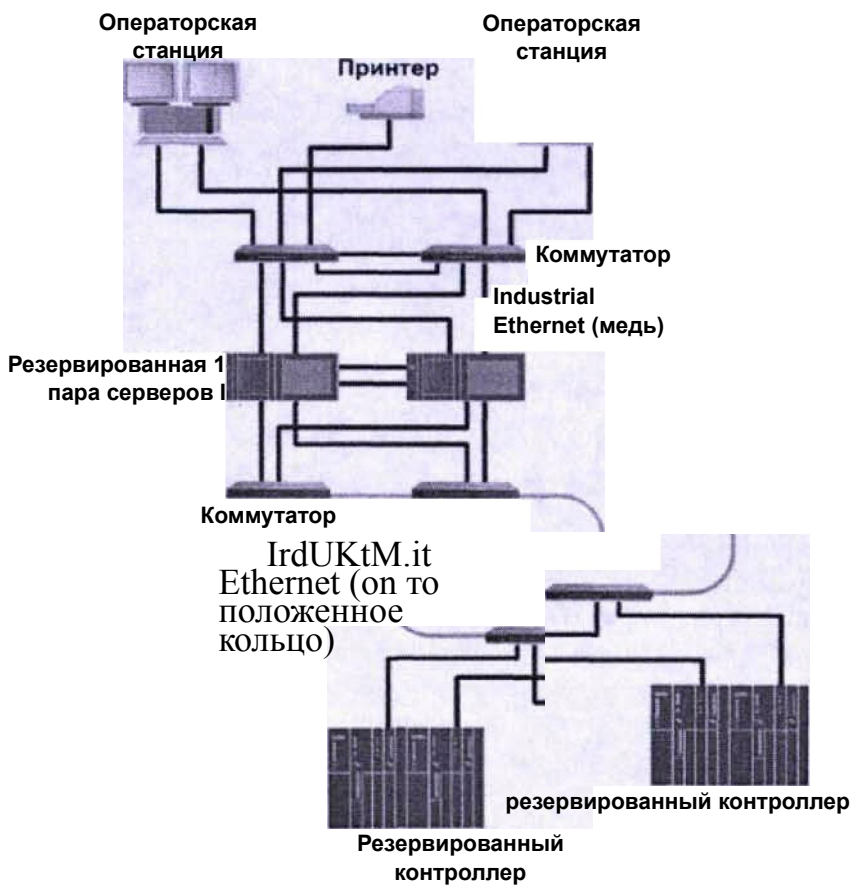


Рисунок 1.9 - Резервированная конфигурация сети на основе оптоволоконного кольца

Мы рассмотрели наиболее типичные схемы построения сетей, применяемых в промышленности. Вместе с тем следует заметить, что универсальных конфигураций сетей попросту не существует: в каждом конкретном случае проектировщик вырабатывает подходящее техническое решение исходя из поставленной задачи и условий применения.

1.6 Выводы и постановка задач

1. Проведен анализ типичных АСУ ТП с точки зрения обеспечения безопасности. Составлена таблица данных о 8 современных АСУ ТП различной степени сложности, внедренных на объектах химического производства и смежных отраслей. Выявлен

дисбаланс в защищенности сетей и оборудования верхнего и нижнего уровней АСУ ТП, требующий исследования и разра-ботки средств и мер защиты сетей и оборудования нижнего уровня АСУ ТП.

2. Проанализированы 12 наиболее распростр

аненных 8САГ)А-систем, применяемых в химической промышленности, и выявлены основные встро-енные механизмы защиты информации. Поскольку в подавляющем большин-стве применений 8САЕ)А-систем используются лишь два метода

защиты: пароли и дублирование оборудования и сетей, то необходимо раскрыть возможности использования средств защиты ЭСАВА-систем совместно со встроенными механизмами защиты сетей и оборудования нижнего уровня АСУ ТП.

3. Иссл
едованы
телекомму
никации,
используе
мые в АСУ
ТП
химическо
й
промышлен
ности,
выявлены
особеннос
ти сетей
нижнего
уровня:
детермин
и-
рованност
ь,
централиз
ованность
,
поддержка
больших
расстояни
й, защита
от
электрома
гнитных

наводок, взрывобезопасность. Не обнаружено сведений о защите телекоммуникаций нижнего уровня АСУ ТП от прямого вторжения. Поэтому целесообразно исследовать информационную безопасность этих те-лекоммуникаций при прямом вторжении и

разработать меры защиты.

4. Выявлено, что проблемы информационной безопасности в химической промышленности обусловлены спецификой производственных процессов: взрывоопасность, пожароопасность, экологическая опасность химическо

го производства, агрессивная среда размещения и рассредоточенность аппаратуры нижнего уровня АСУ ТП. В связи с этим необходимо выявить особенности обеспечения информационной безопасности в АСУ ТП в химической промышлен

ности, провести оценку защищенности телекоммуникаций реальной АСУ ТП от различных угроз.

Исходя из вышеизложенного, можно сформулировать следующие задачи исследования:

- выявить особенности обеспечения информационной

безопасности в АСУ ТП химической промышленности;

- исследовать информационную безопасность телекоммуникаций нижнего уровня АСУ ТП химической промышленности;

- провести экспериментальную проверку защищенности телекомму

никаций нижнего уровня АСУ ТП химической промышленности;

- исследовать эффективность программных методов защиты телеком-муникаций нижнего уровня АСУ ТП химической промышленности;

- провести оценку защищенности

телекомму
никаций
АСУ ТП
«ПХВ-
1»;

- раз
работать
методику
создания
систем
защиты
информаци
и в АСУ
ТП;

- выр
аботать
рекоменда
ции по
обеспечен
ию
информаци
онной
безопас-
ности
телекомму
никаций
нижнего
уровня
АСУ ТП
химическо

й промышленности;

- разработать и проверить алгоритмы обеспечения информационной безопасности телекоммуникаций нижнего уровня АСУ ТП химической промышленности;

- обосновать выбор методов оценки качества

СЗИ в АСУ ТП;

- разработать методику оценки качества СЗИ;

- провести оценку защищенности АСУ ТП «ПХВ-1» по разработанной методике.

2 ЗАЩИТА ИНФОРМАЦИИ В АСУ ТП

Обеспечить информационную безопасность АСУ

ТП на достаточно высоком уровне, при постоянно растущем уровне информатизации и постоянно увеличивающемся количестве угроз, уже невозможно только комплексом внешних мер защиты. Необходим системный подход к обеспечению информационной безопасности АСУ

ТП, когда внешнюю защитную оболочку будет создавать комплексная система информационной безопасности, а внутренние барьеры образуют встроенные механизмы защиты в программных и технических компонентах АСУ ТП.

Обойти

внешнюю защиту можно, внутреннюю — гораздо сложнее. Поэтому автор обращает особое внимание на преимущества разработки и применения программных и аппаратурных средств АСУ ТП, имеющих встроенные механизмы защиты, которыми

пользоват
ель может
управлять
для
создания
требуемой
пропорции
механизмо
в защиты
[14].

Есть
базовый
уровень
обеспечен
ия
информаци
онной
безопасно
сти, ко-
торый
подразуме
вает
обязатель
ное
наличие
определен
ных
средств
защиты.
Так,

например, вирусы представляют опасность для любой информационной системы, поэтому средства антивирусной защиты должны быть всегда. При создании любой информационной системы существует внутренняя политика обеспечения

безопасности, заключающаяся хотя бы в разграничении доступа к ресурсам. Наличие различных прав у разных категорий пользователей вызывает необходимость контроля за реализацией этих прав. Следовательно, обязательно должны быть решены

вопросы аутентификации и наличия механизма администрирования системы. Логично предположить, что если в компании существуют правила и система администрирования, надо ввести некоторый мониторинг процесса функционирования системы, чтобы иметь воз-

можность фиксировать «следы» действий как легальных пользователей, так и нелегальных.

Для обеспечения реализации внутренних правил и регламентов безопасности можно ограничиться

монито
рингом
систем
ы, а с
точки
зрения
внешни
х
воздей
ствий
надо
постар
аться
постав
ить
барьер
для
защиты
от не-
санкци
ониров
анных
действ
ий
извне.
Для
этого
исполь
зуется
,

наприм
ер,
меж-
сетево
й
экран
(firew
all),
опреде
ляющий
права
внешни
х
пользо
вателе
й и
про-
цессов
по
отноше
нию к
внутре
нним.
Это
практи
чески
обязат
ельный
набор,
которы

й
присут
ствует
во
всех
достат
очно
сложны
х
информ
ационн
ых
систе-
мах. А
дальше
начина
ется
другой
уровен
ь,
которы
й
регули
рует
наличи
е и
пропор
ции
тех
или

иных механизмов защиты.

2.1 Особенности обеспечения информационной безопасности в АСУ ТП химической промышленности

Особенностью АСУ ТП в химической промышленности является

ся то, что с их помощью осуществляется управление производственными процессами и системами, от которых непосредственным образом зависит безопасность

и жизнедеятельность нашего общества, а также экологическая обста-новка. Обеспечение информационной безопасности промышленных систем в химической промышленности

требует соответствующего подхода, учитывающего эти особенности. Для того чтобы выработать такой подход, необходимо, прежде всего, оценить серьезность проблемы в

целом, затем, опираясь на накопленную статистику инцидентов, подвергнуть тщательному анализу специфические для промышленных систем угрозы и уязвимости и на основании этого

анализ
а
определ
ить
особые
требов
ания к
режиму
обеспе
чения
ин-
формац
ионной
безопа
сности
критич
еской
инфрас
трукту
ры.
О
беспеч
ение
надежн
ой
защиты
систем
управл
ения
произв

одстве
нными
процес
сами
от
внешни
х
угроз,
таких
как
несанк
ционир
ованны
й
доступ
, ви-
русы,
черви
и
другие
вредон
осные
програ
ммы
жизнен
но
важно.
Пробле
ма
лишь

усилив
ается
из-за
повсем
естног
о
исполь
зовани
я
общепр
инятых
и рас-
простр
аненны
х
станда
ртов и
програ
ммного
обеспе
чения,
таких
как
операц
ионная
систем
а
Micros
oft
Window

s, протокола передачи данных TCP/IP. Атаки систем управления через сети верхнего уровня АСУ ТП, которые зачастую соединены с глобальной сетью, уже давно

не единичны.

Хотя некоторые предприятия установили системы сетевой защиты между системами управления и сетями верхнего уровня АСУ ТП, а также корпоративными сетями, есть многочисленные инциденты, когда хакеры и

черви успешно обходили эту защиту, и использовали уязвимости в самих системах управления технологическими процессами. Существуют и прецеденты, когда подобные атаки были целенаправленными. Экономические последствия подобных

атак могут быть серьезным и, более того возникает угроза жизни лю-дей, а также экологиче ской обстановк е.

Сист емы управлени я становятс я все более уязвимыми. В прошлом системы управлени я разрабаты вались

предприятиями с использованием собст-венных технологий и устанавливались в изоляции от сетей АСУ предпри-ятия, если таковые вообще,имели место быть. Однако, современные тенденции автоматизации требуют использования систем

базирующи
хся на
стан-
дартных
платформа
х
(аппаратн
ых и
программн
ых) из-за
их более
высокой
эффективн
ости и
меньших
затрат.
Кроме
того,
желание
дистанцио
нного
управлени
я и
контроля
привело к
принятию
общих
протоколо
в сети и
созданий

подключен
ий между
многими
из этих
систем к
сетям
АСУП.
Преимуще-
ства
такой
централиз
ации
очевидны,
но к
сожалению
, многие
предприят
ия не в
состоянии
обеспечит
ь и
соответст
вующий
уровень
безопасно
сти таких
сетей.

Боль
шинство
кибер

нападений основываются на прорехах в безопасности систем. Они могут включать в себя:

- **Плохую сегрегацию сети,** другими словами, неполноценное использование брандмауэров, для отделения критических систем от других сетей;
- **Недостаточну**

ю защиту антивирус а — сеть предприят ия не защищена перед вирусам, червям и другим вредоносн ым программн ым обеспечен ием;

- **Неза щищенны е удаленные соединени я** — потенциал ьно предостав ляют свободный доступ хакерам к системам

управлени
я
производс
твенным
процессом
;

- **Пло
хую
физическу
ю
защищенн
ость** –
позволяет
злоумышле
нникам
получать
физически
й доступ
к
системам.
- **Неза
щищеннос
ть
отдаленн
ых
автоматиз
ированны
х рабочих
мест** –
несанкцио

нированны
й доступ
к
системам
управлени
я
производс
твенным
процессом
;

- **Сла
бый
монитори
нг** –
отсутстви
е
своевреме
нного
обнаружен
ия и
оперативн
ого
реагирова
ния на
несанкцио
нированну
ю
деятельно
сть,
такую как

нападение или разведка;

- **Слабую организацию резервного копирования** – отсутствие резервной копии приводит потере важных данных и увеличивает время восстановления работоспособности систем.
- Слабую защищенность паролей к системам.

- **Неустраненные уязвимости в безопасности программного обеспечения** – несвоевременная установка обновлений, обеспечивающих устранение выявленных уязвимостей, предоставляемых производителями программного

обеспечения.

Устранение этих недостатков позволит обеспечить постоянное и безопасное функционирование систем управления и высокую устойчивость к попыткам несанкционированного вредоносного воздействия со стороны

сети верхнего уровня АСУ ТП.

Об особенностях ИТ-инфраструктуры в химической индустрии можно заключить следующее:

- Ни сетевое кабельное оборудование, ни архитектура центров обработки данных, ни каналы связи между различным

и производственными и управленческими площадками, ни какие-либо другие компоненты ИТ-инфраструктуры химического предприятия не имеют отраслевой специфики. Однако химическая отрасль отличается от других отраслей,

например, от металлургической, тем, что помимо крупных предприятий в ней насчитывается множество средних и даже мелких. Соответственно, и особенности информатизации предприятий химической отрасли в значительной степени опреде-

ляются масштабом каждого конкретного предприятия.

- Рабочая среда, в которой функционирует компьютерное оборудование в производственной зоне химического предприятия, часто характеризуется повышенной агрессивностью

(повышенные температура окружающей среды, содержание в воздухе пыли или испарений химически активных соединений и т.д.). Следовательно, компьютерное оборудование и другие компоненты АСУ ТП, работающее в таких условиях, должны иметь

специальное исполнение. При их изготовлении применяют специальные покрытия, антикоррозийные разъемы и внешние корпуса, устойчивые к агрессивному химическому воздействию.

- Повышенное содержание пыли в окружающей среде может

создавать угрозу возгорания. Специализированные компьютерные устройства необходимо снабжать автоматическими средствами пожаротушения. Сопровождающая стекольное производство мелкодисперсная пыль действует как абразив, из-

за чего происходит быстрый износ лопастей вентиляторов и подшип-ников. Чтобы компьютерное оборудование на таком предприятии не вышло из строя до начала регламентных работ, его нужно оборудовать резервными компонентами.

- В инфраструктурных решениях для химической промышленности основное внимание уделяется надежности и функциональным свойствам оборудования и в меньшей степени, по сравнению с обычными коммерческими системами, –

уровню шума, габаритам, весу, дизайну. Все компоненты уст-ройств, используемых на критическом производстве, как правило, должны разрабатываться с запасом прочности, чтобы система обеспечивала приемле-мое время наработки на отказ. Например,

промышлен
ные
системы в
нефте-
химическо
й отрасли
рассчитан
ы на срок
эксплуата
ции не
менее 10-
15 лет.
- Не
все
программн
о-
техническ
ие
решения
могут
быть
использов
аны в АСУ
ТП
химическо
й
промышлен
ности.
Стандарты
промышлен

ной безопас-ности диктуют условия применения тех или иных средств. Для применения в АСУ ТП химической промышленности пригодны специальные промышленные взрыво- и пожаробезопасные решения, соответствующие Российским и

международ
ным
стандарта
м.
Отечестве
нный
стандарт
МЭК
60364-3
устанав-
ливает
требовани
я для
таких
типов
внешних
воздейств
ий, как
проникнов
ение воды
и
посторонн
их
твердых
тел,
механичес
кие удары
и
вибрации,
наличие

химически агрессивных компонентов. Международный стандарт МЭК 529, европейский ЕЙ 60529, французский №0 20-010, немецкие БГМ 40050 и ВШ-УТ)Е 0470 сходным образом определяют код 1Р, где специфицируются степени защиты корпуса электроус

тановки от поражения током, проникновения твердых тел и жидкостей.

2.2 Обеспечение информационной безопасности нижнего уровня АСУ ТП в химической промышленности

2.2.1 Информационная безопасность в аппаратуре и интеллектуальных датчиках

В современных АСУ

ТП всё чаще микропроцессорная техника исполь-зуется на всех уровнях сбора, обработки и исходных данных и выдачи управ-ляющих воздействий [15, 16]

Интеллектуальные датчики [17] обычно строятся на основе

микроко
н-
троллера
,
содержащ
его
аналого-
цифровой
преобраз
ователь,
схемы
возбуж-
дения
датчика
(источни
ки тока,
опорного
напряжен
ия,
генерато
ры
гармони-
ческих
колебани
й).

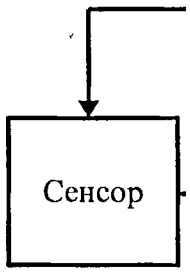


Рисунок 2.1- Структура интеллектуального датчика

Термин «интеллектуальные датчики» был введен для тех первичных устройств, внутри которых содержится микропро

цессор. Обычно это добав- ляет новые функцион альные возможно сти, которых не было в аналогич ных устройст вах без микропро цессора. Например , интеллек туальный датчик может давать более точные показани я

благодаря применению цифровой обработки для компенсации нелинейности чувствительного элемента или температурной зависимости. Интеллектуальный датчик имеет возможность работать с разными типами

чувствительных элементов, а также составлять одно или несколько измерений в одно новое измерение (например, плотность, объемный расход и температуру - в весовой расход). И наконец, интеллектуальный датчик

позволяет производить настройку на другой диапазон измерений или полуавтоматическую калибровку, а также осуществлять функции внутренней самодиагностики, что упрощает техническое обслуживание.

Для связи с верхним уровнем системы управления наиболее рацио-нально использовать цифровой последовательный интерфейс, который обеспечит передачу информации без погрешности, с малой вероятностью иска-жений. Причём цифровая техника

позволяет обнаружив ать и даже исправ- лять наиболее вероятные ошибки. Поэтому будущее за цифровой передачей информаци и.

Одна ко в настоящее время ещё широко использу ется передача инфор- мации от датчиков, в том числе интеллект

уальных, аналоговым унифицированным сигналом постоянного тока [(4...20) мА или (0...5) мА]. Очевидна нецелесообразность такого способа для интеллектуальных датчиков, которые должны опять преобразовать цифровой сигнал в аналоговы

й (с неизбежной погрешностью), передать аналоговый сигнал на некоторое расстояние (с наложением помех) а система верхнего уровня должна снова оцифровать его (и снова с погрешностью).

Способ кажется излишне сложным, но

позволяет осуществлять модер-низацию АСУ ТП. Дело в том, что вместе с современными используется много аналоговых датчиков, для которых аналоговый выходной сигнал является естественным. Системы сбора данных многих действующ

их АСУТП ис-
пользуют
для ввода
информаци
и
многокана
льные
устройств
а ввода
унифи-
цированны
х
аналоговы
х
сигналов
постоянно
го тока,
а не
цифровой
последо-
вательный
интерфейс
. Кроме
того,
регистрир
ующие и
вторичные
показы-
вающие

приборы пока ориентированы больше на аналоговые сигналы датчиков.

Промежуточным решением проблемы излишних преобразований и слабой защищённости аналоговых сигналов при передаче информации, является применение HART-проток

ола (например, датчики давления серии «Метран-100», JUMO dTRANS p02, и другие). Коммуникационный протокол HART® (Highway Addressable Remote Transducer — Адресу

емый Дистанционный Магистральный Преобразователь) специально разработан для обмена данными между системой управления и интеллектуальными первичными датчиками.

Н
ART-
проток
ол
обеспе
чивает
переда
чу
информ
ации и
в
цифров
ой и
аналог
овой
форме
одновр
еменно
по
одной
паре
провод
ов. По
паре
провод
ов
токово
й
петли
(4..20

) мА интелл ектуал ьный датчик , как и обычны й аналог овый, питает ся и переда ёт данные в систем у верхне го уровня измене нием тока в петле. Но интелл ектуал ьный

датчик на медленное изменение тока в петле, пропорциональное измеряемому параметру, накладывает цифровой (бинарный частотный) сигнал малой амплитуды (±0,5 мА). Чаще

всего цифровой обмен информацией производится в режиме настройки датчика, а в режиме измерения используется только аналоговый сигнал. HART-протокол использует станда

рт

BELL

202

кодиро

вки

сигнал

а

методо

м

частот

ного

сдвига

(FSK)<

для

обмена

данным

и на

скорос

ти до

1200

бит/с.

К

аждое

сообще

ние

содерж

ит

адрес

источн

ика и

приёмн
ика, а
также
имеет
контро
льную
сумму
для
обнару
жения
искаже
ний в
сообще
нии.
HART-
проток
ол
постро
ен по
принци
пу
ведущи
й-
ведомы
й.
Ведомы
е (их
может
быть
до 15

штук) только отвечают на запросы ведущего. Но может оказаться двое ведущих (система управления и ручной коммуникатор).

преамбула	стартовый символ	адрес	команда	число байт	статус	данные	контрольная сумма

Рисунок 2.2 - Формат сообщения (кадра) HART-протокола

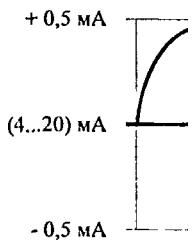


Рисунок 2.3 - Изменение тока в петле с сигналом HART-протокола

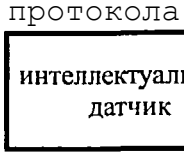


Рисунок 2.4 - Подключение датчика с HART-коммуникатором

Приёмник аналогового сигнала должен иметь фильтр нижних частот, подавляющий

частотн
ый
сигнал
(10 Гц
и
выше),
а
приёмни
к
цифрово
го сиг-
нала
должен
иметь
полосов
ой
фильтр,
выделяю
щий
частоты
бинарно
го сиг-
нала.
Та
кое
решение
сложнее
и
дороже
использ

ования только цифровой передачи, но позволяет осуществить переход на цифровые телекоммуникации постепенно, не затрачивая больших средств на полную замену оборудования АСУ ТП.

Следует рассматривать современные приборы как часть эволюционного развития от аналоговой связи по токовой петле (4...20) мА, через интеллектуальные приборы с одновременно аналого

вой и цифровой связью (HART), до высокостной исключительно цифровой связи с использованием «полевых шин» (fieldbus) в будущем.

2.2.2 Информационная безопасность в АСУ ТП	Расширение сферы цифровой обработки, передачи и хранения информации с одной стороны даёт возможность усилить контроль над целостностью и достове	

рностью информации, а с другой — увеличивает число уяз-вимых мест в системе, особенно при использовании общедоступных каналов связи.

Информационная безопасность (ИБ) представляет собой состояние

за-
щищенност
и
информаци
онной
среды,
обеспечив
ающее ее
формирова
ние,
использов
ание и
развитие.
Осно
вными
техническ
ими
требовани
ями,
обеспечив
ающими
информа-
ционную
безопасно
сть при
проектиро
вании
распредел
енных АСУ

ТП являются:

- обеспечение высоконадежных каналов обмена технологической информацией между отдельными и автоматизированными объектами и централизованной системой управления и контроля;
- защита контрольно-

измерительных и информационных каналов от внешних воздействий, а также усиление передаваемых сигналов;

- обеспечение обмена данными по информационным каналом в реальном масштабе времени;
- резервирование; основной

аппаратуры контроля и управления, а также наиболее важных каналов передачи информации;

- эффективная, с точки зрения скорости обнаружения неисправности, и надежная диагностика программно-аппаратны

х средств;

- обеспечение широкого температурного диапазона работы технических средств локальных систем автоматического управления;
- распределенная система электропитания.

Чаще всего угрозы безопасности являются следствие

м наличия уязвимых мест в системе защиты. Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения

	безопасности.
2.2.2.1	Безопасность использования
	Главной угрозой со стороны пользователей является непреднамеренное нарушение режима работы или настроек интеллектуального датчика.
	Лучшей защитой является введение

пароля доступа к ответственным операциям как с пульта, так и со стороны локальной сети.

Наличие функции восстановления заводских настроек гарантирует быстрое восстановление работоспособности датчика даже при грубых ошибках пользоват

еля.
Аналоговы
й датчик,
кстати,
от
случайног
о
нарушения
настроек
защитить
невозможн
о. Краска
на шлице
потенциом
етра
подстройк
и не
защитит
от
вмешатель
ства, а
восстанов
ить
заводскую
настройку
можно
только в
метрологи
ческой

	лаборатор ии.
2.2.2.2	Безопасно сть аппаратур ы
	Надё жную работу аппаратур ы при сбоях питания, скачках напряжени я и воздейств ии электрома гнитных излучений обеспечит супервизо р питания, а защиту от сбоев программн ого

обеспечения - сторожевой таймер.

Основное назначение супервизора питания (монитора напряжения питания) - обеспечение установки в исходное состояние, перезапуска микропроцессорных или других логических систем при

пониженно
м
напряжени
и во
время
включения
питания,
либо
после
перебоев
подачи
питания
или не-
санкциони
рованного
отключени
я питания
такой
системы.
Супервизо
р не
только
обнаружив
ает
снижение
напряжени
я питания
ниже
допустимо
го уровня

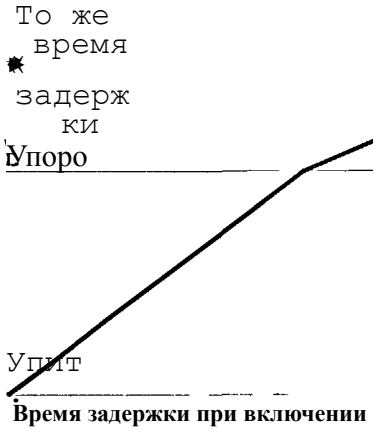
Упорог, но и вырабатывает сигнал системного сброса микроконтроллера RST с фиксированной задержкой (порядка 50 мс для гарантии приведе-ния схем в исходное состояние) после восстановления питания.

Сторожевой таймер (Watch Dog

Timer) представляет собой независимый встроенный генератор, не требующий никаких внешних цепей. Он работает, даже если основной тактовый генератор остановлен. Если сторожевой таймер не сбрасывать, то по истечении заданной выдержки времени (обычно

от 20 мс до 2 с) он вырабатывает сигнал системного сброса микроконтроллера, и таким образом автоматически перезапускает программу. Микрокон-троллеры всегда работают по циклическим программам, с обычным периодом от 0,1 мс

до 1 с, и по программе регулярно обнуляют сторожевой таймер. Поэтому выработка сторожевым таймером сигнала системного сброса является аварийной ситуацией, свидетельствующей о сбое исполнения програм-мы.



Время задержки при включении

RST

Рисунок 2.5 - Принцип работы супервизора питания

Интеллектуальные датчики потребляют мало энергии, поэтому несложно организовать питание

по информационной линии (например, удалённые датчики температуры DS1820 с однопроводным интерфейсом MicroLAN [19]) или резервное батарейное питание.

Из всего оборудования АСУ ТП интеллектуальные датчики наиболее

подвержен
ы
воздейств
ию
окружающе
й среды,
так как
должны
располага
ться
вместе с
первичным
преобразо
вателем
непосредс
твенно на
объекте
управле-
ния. На
интеллект
уальный
датчик
могут
воздейств
овать
экстремал
ьные тем-
пературы,
вибрация,
агрессивн

ые газы и жидкости, взрывоопасные смеси. Поэтому должна использоваться электроника промышленного исполнения с диапазоном рабочих температур не менее (-40...+85) °С; низкое напряжение питания, желательно не более 1,8 В, для

облегчения выполнения требований искробезопасности. Корпуса для интеллектуальных датчиков должны быть антивандальными, а также иметь защиту от пыли и воды (для применения во взрывоопасных зонах согласно главе 7.2 ПУЭ - не

ниже

IP54).

Все вышеперечисленные средства применяются де факто в новых промышленных интеллектуальных датчиках [18]. Например, датчики давления ПД-1ЦМ и температуры ТЦ-1М (ЗАО «НПП «Автоматика», г. Владимир),

датчик давления MPM4760 (MicroSensor, Китай), dTRANS p02 (JUMO, Германия), и другие.

2.2.2.3 Безопасность программного обеспечения датчиков

Разработчики приборов стремятся использовать все возможности микропроцессорной техники, в частности возможность модернизации программного обеспечения в процессе эксплуатации. Это стало возможно с появлением и широким распространением микроконтроллеров, программируемых в системе, и микроконтроллеров, способных производить запись в собственную память программ. Раньше микроконтроллер можно было перепрограммировать, только изъяв его из системы, в специальном программаторе. В микроконтроллере отсутствовали команды записи в память программ, как говорится, по определению.

Обновление программного обеспечения микроконтроллера может производиться как с помощью местного компьютера, так и через интернет. Наиболее удобным и наиболее опасным как для потребителя, так и для производителя, является размещение обновлённых программ на сайте производителя. В этом случае достоверность и целостность программ подвержены наибольшему риску.

2.2.2.4 Безопасность при обмене информацией

Проблема безопасности обмена информацией между интеллектуальными датчиками и системой верхнего уровня менее проработана.

При обмене информацией между интеллектуальными датчиками и системой верхнего уровня используются только физический уровень, уровень передачи данных и прикладной уровень семиуровневой модели взаимодействия открытых систем (OSI).

- Физический уровень (Physical Layer) обеспечивает необходимые механические, функциональные и электрические характеристики для установления, поддержания и размыкания физического соединения.

• Уровень передачи данных (Data Link Layer) гарантирует передачу данных между устройствами. Этот уровень управляет не только сетевым доступом, но также механизмами защиты и восстановления данных в случае ошибок при передаче.

• Прикладной уровень (Application Layer Inferface) обеспечивает непосредственную поддержку прикладных процессов и программ конечного пользователя и управление взаимодействием этих программ с различными объектами сети передачи данных.

Все другие уровни, как правило, избыточны. Перечисленных уровней достаточно в силу ограниченной длины посылок и фиксированной топологии сети датчиков. Защита нижнего (физического) уровня, заключающаяся в проверке чётности при передаче байта, не используется, так как имеется защита на уровне передачи данных. На уровне передачи данных контролируются функции (команды) на допустимость, длина посылки и контрольная сумма после передачи каждого кадра информации перед использованием этой информации. Метод контроля корректности передаваемых данных основан на получении подтверждения (квитирования) получения сообщения. Ведущий также контролирует время до прихода ответа ведомого (тайм-аут), чтобы обнаружить отказы ведомого или соединений локальной сети. Ведомый переводит свои выходы в режим ожидания, если время до прихода очередного запроса превысит допустимый тайм-аут.

В защищённых профилях (например, FailSafe-профиль Profibus) функции обеспечения безопасности реализуются на программном уровне, расположенном выше 7 уровня модели OSI. Контроль корректности расширен за счёт удлинения кадров, но это существенно снижает пропускную способность канала. Для преимущественно коротких сообщений лучше обратить внимание на более защищённую среду передачи — экранированный кабель, коаксиальный кабель или оптоволокно.

Многие «внутренние», закрытые протоколы, например, протоколы ОВЕН, МЗТА, МЕТАКОН не получили распространения за пределами сетей приборов соответствующих фирм-производителей (Овен, МЗТА, КонтрАвт) в частности и потому, что для упрощения и ускорения обмена не все элементы защиты предоставляют.

В настоящее время в химической промышленности чаще всего используются промышленные локальные сети Modbus RTU/ASCII и Profibus DP/PA, входящие в семейство «полевых шин» (fieldbus) и работающие по принципу доступа к единой шине: «один ведущий, а остальные узлы сети — ведомые» (централизованное управление). В некоторых других «полевых шинах»: Profibus FMS, CANopen, DeviceNet, - любой узел может быть ведущим (децентрализованное управление). Каждый принцип имеет преимущества и недостатки. Сравним эти сети с точки зрения обеспечения информационной безопасности.

Modbus RTU/ASCII и Profibus DP на физическом уровне используют интерфейс RS-485 на скоростях до 115,2 Кбит/с и 12 Мбит/с, соответственно. Кадры посылок иллюстрируют Рисунок 2.6 и Рисунок 2.7.

адрес приёмника (ведомого устройства)	номер функции	данные	контрольная сумма	разделитель сообщений
1 байт	1 байт	до 253 байт	2 байта	пауза >3,5 байт

Рисунок 2.6 - Кадр посылки Modbus RTU

стартовый разделитель	адрес приёмника	адрес пере-датчика	номер функции	данные	контрольная сумма	столовый разделитель
1 байт	1 байт	1 байт	1 байт	до 244 байт	2 байта	1 байт

Рисунок 2.7 - Кадр посылки Profibus

Поля «данные» - это полезная информация; «адрес», «номер функции», «разделитель сообщений» - это служебная информация; «контрольная сумма» - это программная защита.

Вмешаться в сеть с одним ведущим электрически возможно, достаточно подключиться к паре проводов локальной сети в любом месте. Но при этом явно нарушается протокол — возникает второй ведущий. Наложение сигналов запроса дополнительного ведущего на периодический запрос штатного ведущего приведёт к сбою процедуры обмена, и такая посылка не пройдёт. Если запрос дополнительного ведущего и ответ пройдут в промежутке между процедурами обмена штатного ведущего, то эти посылки будут приняты и штатным ведущим. В этом случае необходимо предусмотреть соответствующую реакцию штатного ведущего на вмешательство в сеть! Так как в самом протоколе локальной сети не предусмотрено мер, кроме занесения возникшей ситуации в счётчик сбоев обмена.

Вмешаться в сеть со многими ведущим проще, так как при этом даже не нарушается протокол. Возникновение и разрешение конфликтов при захвате магистрали — нормальная процедура для такой сети. Поэтому уязвимость такой сети значительно выше [20]. Конечно, есть способ борьбы с вмешательством в сеть со многими ведущими. Он заключается в фиксации числа и адресов штатных узлов в конкретной сети. Так рекомендуют делать, например, в АСУТП атомных станций [21]. Однако такое решение лишает систему гибкости и требует вмешательства квалифицированного программиста на уровне операционной системы.

Централизованный доступ по сравнению с децентрализованным обеспечивает больший уровень безопасности, поэтому, в частности, подавляющее большинство промышленных сетей построены по принципу централизованного доступа [22].

Ограничение доступа к локальной сети возлагается на 8САОА-систему, собирающую информацию с датчиков, и на операционную систему, в которой функционирует БСАБА-система. Типовая 8САБА-система для этого обеспечивает:

- Разграничение прав доступа пользователей и защиту паролями.

- Удаленную перезагрузку ведомых узлов сети.
- Исполнение функций сторожевого таймера.
- Автоматическое тестирование коммуникаций, обнаружение ошибок.
- Выдачу информации об ошибках коммуникации.
- Восстановление исходных настроек параметров ведомых узлов и коммуникаций.

Полный перечень защитных механизмов 8САЭА-систем приводится в Приложении 2. Из этого перечня видно, что универсальные 8САХ)А-системы имеют полный набор средств защиты, которые можно задействовать в нужной комбинации для конкретного применения.

Многие «внутренние» БСАОА-системы, например, фирм КонтрАвт, ОВЕН, МЗТА не получили распространения за пределами сетей приборов соответствующих фирм-производителей из-за несовместимости с оборудованием и программами других фирм и неполного набора средств защиты. **2.3 Рекомендации по выбору интеллектуальных датчиков, и локальных** сетей для них

В данной главе рассмотрены проблемы обеспечения информационной безопасности на нижнем уровне АСУ ТП в связи с применением интеллектуальных датчиков. На основании анализа продукции многих производителей можно сделать выводы, которые полезны не только проектировщикам АСУ ТП, но и разработчикам интеллектуальных датчиков.

Для защиты информации в АСУ ТП следует обращать внимание на выполнение следующих требований к интеллектуальным датчикам:

- наличие функций внутренней самодиагностики датчиков, что упрощает техническое обслуживание;
- избыточность измерений и кодирования, позволяющая обнаруживать и даже исправлять наиболее вероятные ошибки;
- высокоскоростная и исключительно цифровая связь с использованием «полевых шин»;

• разграничение прав доступа пользователей и наличие паролей доступа к ответственным операциям как с пульта, так и со стороны локальной сети;

• наличие функции восстановления заводских настроек гарантирует быстрое восстановление работоспособности датчика даже при грубых ошибках пользователя;

• наличие супервизора питания обеспечивает надёжную работу аппаратуры при сбоях питания, скачках напряжения и воздействии электромагнитных излучений обеспечит и сторожевого таймера защиту от сбоев программного обеспечения;

• использование электроники промышленного исполнения с широким диапазоном рабочих температур, низким напряжением питания, желательно не более 1,8 В, для облегчения выполнения требований искробезопасности;

• антивандальный корпус с защитой от пыли и воды не ниже 1Р54 для применения во взрывоопасных зонах согласно главе 7.2 ПУЭ;

• питание по кабелю локальной сети или по информационной линии, возможно с резервным батарейным питанием;

При выборе промышленной локальной сети для АСУ ТП важен набор критериев, по которым можно сделать осмысленный выбор того или иного протокола [23]:

• Централизованный доступ: сеть должна быть с одним «ведущим», что обеспечит больший уровень безопасности.

• Контроль корректности передаваемых данных: проверка допустимости команд, длины посылок, контрольных сумм, квитирование сообщений и т. п.

• Открытость: прежде всего, отсутствие лицензионной платы за использование протокола в своих разработках.

• Информативность: насколько доступны спецификации протоколов и стандарты, на которые опираются эти протоколы.

• Перспективность: насколько тот или иной протокол допускает возможность развития и как он приспосабливается под нужды потребителей.

• Информационная поддержка в стране: документация на русском языке, ассоциации пользователей, в которой можно получить исчерпывающие ответы на вопросы.

Первые два критерия, к сожалению, не присутствуют среди критериев оценки сетей, приведённых в [23].

Возможность применения Интернета для управления технологическими процессами пока под большим вопросом [24]. Есть, по крайней мере, две причины, которые препятствуют этому.

Во-первых, хакеры.

Во-вторых, для систем управления технологическими процессами важно гарантированное время доставки управляющих воздействий, а Интернет не гарантирует время доставки.

2.4 Разработка методики создания систем защиты информации в АСУ ТП

Поскольку с каждым годом вопросы обеспечения информационной безопасности АСУ ТП приобретают всё большее значение, рассмотрим методологию создания систем защиты АСУ ТП.

АСУ ТП отличается от других систем управления прежде всего тем, что осуществляет воздействие на объект в том же темпе, что и протекающие в нём технологические процессы, а технические средства АСУ ТП участвуют в выработке решений по управлению. Первая особенность требует применения в АСУ ТП телекоммуникаций с гарантированным временем доставки, вторая — интеллектуализации всех компонентов от датчиков до исполнительных механизмов.

В иерархической многоуровневой архитектуре современной АСУ ТП нижний уровень характеризуется большим количеством (сотни) и разнообразием технических средств, которые различаются также информационным, математическим и программным обеспечением.

Предприятия химической отрасли разномасштабные (малые, средние и крупные) и обладают, кроме общепромышленной специфики, взрывоопасно- стью, пожароопасностью, агрессивностью рабочей среды, воздействием на экологию и жизнедеятельность общества даже в штатном режиме работы.

Учитывая эти особенности, попытаемся определить общие и особые требования к режиму обеспечения информационной безопасности АСУ ТП [3, 25].

Основными потенциально возможными угрозами [6] физической целостности информации, т.е. стирание или модификация (искажение) информации на носителях и документах, используемых в процессе функционирования АСУ ТП, являются следующие:

- Сбои и отключение питания.
- Прямое физическое воздействие на носители или документы.
- Законное или несанкционированное подключение к аппаратуре и линиям связи.

Защита информации в плане уязвимости первого вида заключается в основном в применении надежной, физически и энергозащищенной аппаратуры и в обеспечении ограничения доступа к ней.

Основными потенциально возможными каналами утечки информации являются следующие:

- Прямое хищение носителей и документов, обращающихся в процессе функционирования АСУ ТП.
- Запоминание или копирование информации, находящейся на машинных и на немашинных носителях.
- Несанкционированное подключение к аппаратуре и линиям связи или незаконное использование «законной» (т. е. зарегистрированной) аппаратуры системы (чаще всего терминалов пользователей).
- Несанкционированный доступ к информации за счет специального приспособления, математического и программного обеспечения.

При наличии такого количества каналов утечки необходимы специальные средства, методы и мероприятия, предназначенные для перекрытия перечисленных каналов и предупреждения этим несанкционированного использования информации.

В создании и обеспечении функционирования таких средств, методов и мероприятий и заключается защита информации в плане уязвимости второго вида.

Особое внимание нужно уделить живучести АСУ ТП. Живучесть АСУ ТП обеспечивается:

- применением надёжной аппаратуры и проверенного ПО,
- непрерывным контролем в процессе эксплуатации,
- периодическим тестированием во время технологических остановок,
- адаптивными алгоритмами контроля и управления,
- системой обновления ПО в процессе эксплуатации,
- экранированием сигнальных цепей и источников помех,
- применением интеллектуальных датчиков и исполнительных узлов,
- бесперебойным энергообеспечением.

Рассмотрим типовую трехуровневую структуру АСУ ТП. На верхнем уровне находятся рабочие станции (компьютеры со специализированным ПО, объединённые в локальные сети), на среднем уровне — групповые контроллеры, обеспечивающие групповое управление, на нижнем — локальные контроллеры и устройства управления технологическим процессом. В Таблице 2.1, составленной автором в результате исследования ряда АСУ ТП в химической промышленности (Приложение 1, Приложение 2) представлен перечень мер по обеспечению информационной безопасности на всех уровнях типовой трехуровневой модели АСУ ТП.

Таблица 2.1 - Обеспечение безопасности АСУ ТП на всех уровнях	Рабочие (операторские) станции	Горячее резервирование станций. Резервирование узлов станции (жесткий диск, контроллеры ЛВС, питание и т.д.) Защита от несанкционированного доступа к системе и данным. Защита от вредоносного программного обеспечения. Защита каналов связи ЛВС. Использование межсетевых экранов.
Верхний уровень		

Групповой (средний) уровень	Многоканальные (групповые) контроллеры	Работа с несколькими локальными сетями и защита доступа. Горячее резервирование контроллеров. Косвенный контроль каналов, датчиков, исполнительных механизмов по связанным параметрам. Обеспечение безударного перехода на резервный канал, или на ручное управление (и обратно). Применение интеллектуальных УСО.
Нижний уровень	Локальные контроллеры	Работа в локальной сети и защита доступа. Самодиагностика (сетей, аппаратуры, программ). Генерирование тест-сигналов и анализ их воздействия. Запоминание текущего состояния при сбоях питания и плавный вход в регулирование после восстановления питания. Обеспечение безударного перехода на ручное управление (и обратно). Тестирование измерительных преобразователей (линий связи).
	Исполнительные механизмы с системой управления	Контроль пусковых режимов (защита от перегорания). Защита от длительной перегрузки (тепловой и косвенный контроль). Применение датчиков положения исполнительных механизмов. Дублирование для аварийной защиты. Автоматический возврат в безопасное состояние при исчезновении питания или управляющего сигнала. Бесперебойное питание (по крайней мере, аварийных механизмов)
	Измерительные преобразователи	Тестирование сенсоров (линий связи) непрерывно или циклически. Сравнение результатов измерения с физически возможными. Оценка достоверности с помощью косвенных измерений по связанным параметрам. Искробезопасное питание от локальных или групповых контроллеров. Горячее резервирование.
	Сенсоры	Надёжные, тестируемые, изолированные сенсоры.

Эффективность механизмов защиты информации в значительной степени зависит от реализации ряда принципов. Во-первых, механизмы защиты следует проектировать одновременно с разработкой информационно- управляющей системы, что позволяет обеспечить их бесконфликтность, своевременную интеграцию в вычислительную среду и сокращение затрат. Во-вторых, вопросы защиты следует рассматривать системно, дополняя наружную защиту встроенными механизмами защиты компонентов АСУ ТП. И, наконец, следует учитывать тот факт, что промышленные системы создаются для длительной эксплуатации без

замены или модернизации. Поэтому проверка эффективности СЗИ должна быть произведена в начале промышленной эксплуатации.

Предлагаемый автором системный подход обеспечивает адекватную многоуровневую защиту информации, рассматриваемую как комплекс организационных и технических мероприятий. Кроме того, при реализации механизмов защиты должны использоваться передовые, научно обоснованные технологии защиты, обеспечивающие требуемый уровень безопасности, приемлемость для пользователей и возможность наращивания и модификации СЗИ в дальнейшем.

Создание систем безопасности АСУ ТП охватывает широкий круг вопросов, в число которых входит:

- обеспечение целостности,
- обеспечение конфиденциальности и аутентичности информации;
- разграничение прав пользователей по доступу к ресурсам автоматизированной системы;
- защита автоматизированной системы и ее элементов от несанкционированного доступа;
- обеспечение живучести всех элементов системы;
- защита поддерживающей инфраструктуры системы.

Построение защищенных систем не ограничивается выбором тех или иных аппаратных и программных средств защиты. Необходимо владеть определенными теоретическими знаниями и практическими навыками. Для этого необходимо, во-первых, понять, что представляет собой защищенная система, какие к ней предъявляются требования, рассмотреть существующий опыт создания подобных систем и причины нарушения их безопасности и, во-вторых, определить, какие функции защиты и каким образом должны быть реализованы, и как они противодействуют угрозам и устраняют причины нарушения информационной безопасности [26, 27, 28, 29].

Основой или составными частями любой автоматизированной системы (в том числе и системы защиты информации АСУ ТП) являются:

- Нормативно-правовая и научная база;

- Структура и задачи автоматизированной системы;
- Организационные меры и методы;
- Программно-технические способы и средства.

Далее следует выделить основные направления в общей проблеме обеспечения информационной безопасности АСУ ТП:

- Защита объектов автоматизированной системы;
- Защита процессов, процедур и программ обработки информации;
- Защита информации в каналах связи;
- Подавление побочных электромагнитных излучений;
- Защита поддерживающей инфраструктуры;
- Управление системой защиты.

Разработанная автором методика (последовательность шагов) построения СЗИ (Рисунок 2.8), которая в равной степени применима для всех направлений защиты АСУ ТП, предполагает следующую последовательность действий, основанную на системном подходе и учитывающую особенности АСУ ТП и химической промышленности [32]:

1. Изучение нормативно-правовой и научной базы в области информационной безопасности применительно к промышленным системам повышенной опасности.
2. Определение информации, подлежащей защите в рабочих станциях, контроллерах, телекоммуникациях, устройствах сопряжения с объектом.
3. Выявление полного множества потенциально возможных угроз и каналов утечки информации в штатном, предаварийном и аварийном режимах работы АСУ ТП.
4. Составление реестра встроенных механизмов защиты аппаратных и программных средств АСУ ТП, не препятствующих её работе в темпе процесса.
5. Проведение экспертной оценки уязвимости информации и рисков при имеющемся множестве угроз и каналов утечки.
6. Определение требований к СЗИ с учётом использования встроенных механизмов защиты.

7. Включение встроенных и выбор внешних средств защиты информации и их характеристик.

8. Оформление документации на СЗИ как на подсистему АСУ ТП.

9. Внедрение и организация использования выбранных мер, способов и средств защиты.

10. Осуществление контроля целостности и управление СЗИ в течение всего срока эксплуатации.

Указанная последовательность действий должна осуществляться непрерывно по замкнутому циклу, с проведением оперативного анализа (силами разработчиков) состояния СЗИ АСУ ТП и уточнением требований к ней после каждого шага. Экспертная оценка уязвимости информации и рисков необходима как до создания СЗИ (блок 5), так и после её внедрения (блока 9).

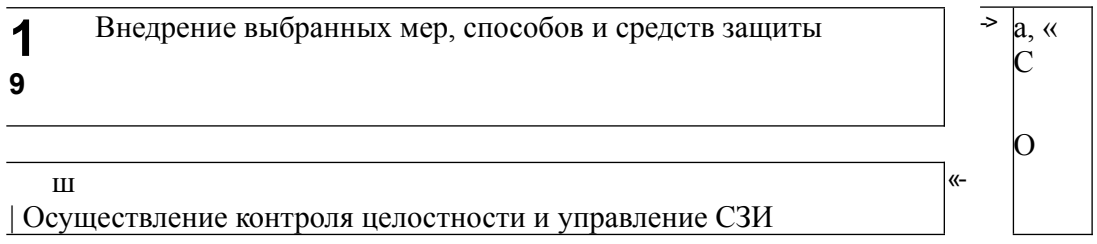


Рисунок 2.8 - Методика построения СЗИ. Непрерывный цикл создания системы защиты информации в АСУ ТП

Применяя данную методику необходимо помнить что наибольший эффект достигается тогда, когда:

- все используемые средства, методы и мероприятия объединяются в единый, целостный механизм защиты информации;
- механизм защиты должен проектироваться параллельно с созданием систем обработки данных, начиная с момента выработки общего замысла построения системы;
- функционирование механизма защиты должно планироваться и обеспечиваться наряду с планированием и обеспечением основных процессов автоматизированной обработки информации;
- необходимо осуществлять постоянный контроль функционирования механизма защиты.

2.5 Выводы

1. Рекомендовано, наряду с комплексом внешних мер защиты, которые в 8САХ)А-системах ограничиваются системой паролей и дублированием каналов и оборудования, применять на нижнем уровне АСУ ТП аппаратурные компоненты и программные продукты, имеющие встроенные механизмы защиты информации. Алгоритмы работы этих механизмов защиты необходимо исследовать, оценить и доработать.

2. Выработаны рекомендации по выбору интеллектуальных датчиков, и локальных сетей для них.

3. Обосновано использование универсальных 8САОА-систем, имеющих полный набор встроенных средств защиты, которые можно задействовать в нужной комбинации для конкретного применения.

4. Обоснованы особые требования к аппаратуре и телекоммуникациям АСУ ТП в химической индустрии. В дополнение к существующим международным стандартам, определяющим только базовые механизмы безопасности, рекомендовано применять также специализированные стандарты и руководства.

5. Разработана методика создания СЗИ в АСУ ТП.

3 ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИЯХ АСУ ТП

Особенности сложных АСУ ТП большой размерности привели к тому, что главной проблемой оценки их надежности и безопасности давно стали не расчеты показателей, а громоздкость и трудоемкость процессов построения необходимых математических моделей. Невозможность построения таких моделей старыми, традиционными ручными (не автоматизированными) технологиями привела к тому, что в организациях и на предприятиях промышленности практическое моделирование и оценка надежности и безопасности АСУ ТП давно не производится ни на стадиях проектирования, ни в процессе эксплуатации [31, 33].

Однако при оценке информационной безопасности АСУ ТП, особенно на нижнем уровне, где используются сети с централизованным детерминированным доступом, можно обойтись очень простыми моделями. В силу детерминированности в них не требуется имитировать и генерировать потоки заявок на захват магистрали и анализировать время ожидания обслуживания. Случайной является лишь длина кадров. Причём, если рассматривать режим настройки отдельно от режима эксплуатации, то распределение длин посылок с сети близко к экспоненциальному. Наиболее вероятны самые короткие посылки. Длина посылок увеличивается для многоканальных узлов. А число повторных запросов (при исключительных ответах) в основном зависит от вероятности битовых ошибок (фактически от уровня помех).

Уровень безопасности телекоммуникационной системы сильно зависит от конкретной физической среды передачи. Таблица 3.1 содержит эту зависимость в виде значений вероятности битовой ошибки для различных физических сред передачи [33].

Таблица 3.1 - Безопасность различных сред передачи Вероятность ошибки передачи бита	Среда передачи

информации	
> КГ[5]	Радиоканал
10"[4]	Неэкранированный кабель
10°	Экранированная витая пара
10"[ь]- 10"[у]	Цифровой канал ISDN
10"[у]	Коаксиальный кабель
Ю-[12]	Оптический кабель

Таблица 3.1 приведена только для сравнительно оценки уязвимости сред передачи, без каких-либо мер защиты.

3.1 Оценка производительности телекоммуникаций в АСУ ТП

Прежде, чем рассматривать пригодность моделей информационных сетей, сформулируем требования к их назначению, сфере использования, а главное — ко входным и выходным параметрам.

Модели предназначаются для анализа уязвимостей и воздействия угроз на телекоммуникации в АСУ ТП, и должны показывать влияние средств и мер защиты от разного рода неблагоприятных воздействий на информацию.

Модели должны отображать влияние средств и мер защиты на достоверность и своевременность передачи и приёма информации, прежде всего на пропускную способность телекоммуникаций.

Модели информационных сетей с одним ведущим проще в связи с тем, что не требуется анализировать процессы захвата магистрали, распределения вероятностей запросов, время ожидания и т.п. В сетях с одним ведущим запросы вырабатывает головной компьютер (контроллер) по жёсткому графику.

Степень влияния мер защиты, особенно программных, на пропускную способность телекоммуникаций существенно зависит от распределения вероятностей длины сообщений. Количество дополнительных (защитных) байт и для коротких и для длинных сообщений одинаково, поэтому избыточность коротких сообщений существенно больше.

Выбор модели определяется целью моделирования. В нашем случае необходимо анализировать влияние средств и мер защиты информации на основные характеристики телекоммуникаций.

Основными техническими средствами защиты являются физическая среда передачи информации: медный провод, кабель, радиоканал или оптоволокно. Таблица 3.1 показывает, что самый низкий уровень защищённости предоставляет радиоканал, а самый высокий — оптоволокно. Вероятность ошибки передачи бита информации из Таблица 3.1 служит для расчёта вероятности повторных запросов, т.к. однократные ошибки при передаче данных обнаруживаются на канальном уровне с помощью СЯС-кода.

Основным программным способом защиты информации в телекоммуникациях является избыточное кодирование, сводящееся к добавлению контрольных битов, контрольных сумм, использованию служебных параметров. Поэтому для анализа влияния средств и мер защиты информации целесообразно рассчитывать следующие параметры сети:

Скорость в кабеле (максимальная скорость передачи пакетов):

$8_К = \$_{MAX} / У_п$ [пакет/с], (3.1.1)

где Б max - предельная скорость сети, бит/с; Уп - длина пакета, бит.

Пропускная способность сети представляет собой скорость передачи полезной информации:

8с = 8к/Уд [байт/с], (3.1.2)

где Бк - максимальная скорость передачи пакетов, пакет/с; $У_д$ - объём полезной информации в пакете, байт.

Эффективность использования физической скорости передачи сети по отношению только к полезным данным:

$Э_д = 8_К$ х $У_д$ / $8_{мах}$ [%], (3.1.3)

где 8к - максимальная скорость передачи пакетов, пакет/с; 8мах - предельная скорость сети, бит/с; Уд - объём полезной информации в пакете, бит.

Вероятностный подход позволяет легко оценить влияние случайных воздействий на приведённые выше параметры. При наличии помех или сбоев передачи данных по другим причинам, эффективность использования физической скорости передачи сети снижается за счёт генерации повторных запросов.

3.2 Оценка мер защиты телекоммуникаций в АСУ ТП

Программные меры защиты основаны на введении избыточности кодирования сообщений. В каждом сообщении кроме обязательной служебной информации (адрес приёмника, функция, номер и количество регистров, разделитель) содержится защитная информация (контрольная сумма, количество байт данных, адрес источника, и ответное сообщение - как квитанция приёма).

Подсистема обеспечения надежности современных SCADA-систем позволяет диагностировать достоверность (качество) сигналов, поступающих с датчиков и резервировать их. Признаки аппаратурной и программной достоверности должны передаваться в систему верхнего уровня (SCADA-систему) вместе с измеренным значением как один из атрибутов канала, чтобы их можно было использовать в алгоритмах диагностики и резервирования датчиков.

Для оценки эффективности стандартной защиты при передаче коротких сообщений, характерных для сетей нижнего уровня АСУ ТП, рассмотрим наиболее распространенные в химической промышленности сети: Ethernet, Modbus, Profibus.

3.2.1 Оценка производительности сети Ethernet

Сеть Ethernet чаще всего используется на верхнем уровне АСУ ТП для связи с АСУ предприятия и для связи рабочих станций между собой [34].

Вопрос об оценке производительности сетей децентрализованного доступа, использующих случайный метод доступа CSMA/CD (Carrier-Sense Multiple Access with Collision Detection - множественный доступ с контролем несущей и обнаружением коллизий), не очевиден из-за того, что существуют

несколько различных показателей. Прежде всего, следует упомянуть три связанные между собой показателя, характеризующие производительность сети в идеальном

случае — при отсутствии коллизий и при передаче непрерывного потока пакетов, разделенных только межпакетным интервалом IPG. Очевидно, такой режим реализуется, если один из абонентов активен и передает пакеты с максимально возможной скоростью. Неполное использование пропускной способности в этом случае связано, кроме существования интервала IPG, с наличием служебных полей в пакете Ethernet.

Пакет максимальной длины является наименее избыточным по относительной доле служебной информации. Он содержит 12304 бит (включая интервал IPG), из которых 12000 являются полезными данными.

Поэтому максимальная скорость передачи пакетов (3.2.1) составит в случае сети Fast Ethernet:

10^8 бит/с/ 12304 бит ~ 8127,44 пакет/с.

Пропускная способность равна:

8127,44 пакет/с х 1500 байта - 12,2 Мбайт/с.

Эффективность использования физической скорости передачи сети, в случае Fast Ethernet равной 100 Мбит/с, по отношению только к полезным данным составит:

8127,44 пакет/с х 12000 бит/ 10^8 бит/с ~ 98 %.

Без использования системы никакой из абонентов не может захватить сеть более чем на время передачи одного пакета, однако передача данных отдельными пакетами с долгими паузами между ними ведет к снижению скорости передачи для каждого абонента. Преимущество детерминированных методов состоит в возможности простой организации системы приоритетов, что полезно из-за наличия иерархии в любой АСУ ТП.

3.2.2 Анализ влияния программных мер защиты в сети Modbus RTU Проведем анализ стандартных программных мер защиты информации в сети Modbus RTU, при использовании её в АСУ ТП. Сеть Modbus является централизованной, с детерминированным методом доступа. Загрузку такой сети можно рассчитать достаточно точно, если определено количество узлов и режимы их работы. Случайный характер имеет лишь время задержки ответа ведомого, а также количество сбоев обмена.

Рисунок 3.1 представляет обобщённый формат кадра:

адрес приёмника (ведомого устройства)	номер функции	данные	контрольная сумма	разделитель сообщений
1 байт	1 байт	до 253 байт	2 байта	пауза > 3,5 байт

Рисунок 3.1 - Кадр Modbus RTU

Передача каждого байта данных требует дополнительно 1 стартового и 2 стоповых битов (без контроля на чётность). Дополнительные биты относятся к служебным, они обеспечивают синхронизацию обмена.

В АСУ ТП интеллектуальные датчики подавляющую часть времени отвечают на циклические запросы SCADA-системы о значении измеряемого параметра, а именно, на запросы «Чтение значений из нескольких регистров». Поскольку для SCADA-системы нужны значения измеряемого параметра в формате Float 4 (Float Single Format no IEEE-754), занимающем 2 регистра (4 байта), конкретные циклы обмена информацией выглядят как показывает Рисунок 3.2.

Запрос ведущего устройства:

адрес • ведомого	номер функции	Адрес ст. байт	Адрес мл. байт	Кол. регистров ст. байт	Кол. регистров мл. байт	CRC мл. байт	CRC ст. байт
0x01	0x03	0x00	0x01	0x00	0x02	OxNN	OxNN

Ответ ведомого устройства:

адрес ведо-мого	номер функции	Кол. байт	Данные ст.регистра ст.байт	Данные ст.регистра мл. байт	Данные мл.регистра ст.байт	Данные мл.регистра мл.байт	CRC мл. байт	CRC ст. байт
0x01	0x03	0x04	0x12	0x34	0x56	0x78	OxNN	OxNN

Рисунок 3.2 - Цикл обмена информацией с одноканальным узлом сети МосШиэ ЯТи Таким образом, необходимой для исполнения команды считывания данных информацией является «адрес ведомого», «номер функции», «адрес первого регистра», «количество регистров» в запросе и собственно «данные» в ответе. Всего 10 байт. Запрос, ответ и минимальная пауза между ними составляют 20,5 байт. Очевидно, что введение защиты в форме избыточности кодирования, т.е. добавления полей «контрольная сумма CRC», «количество байт данных», квитанций «адрес ведомого» и «номер функции», - приводит к снижению пропускной способности канала на 51 %:

ЮОх (10 - 20,5)/20,5 = - 51,22 %.

3.2.2.1 Кадр максимальной длины является наименее избыточным по относительной доле служебной информации (см. Рисунок 3.1). В Modbus RTU он содержит 2084 бит (включая разделительную паузу), из которых 2016 бит являются полезными данными.

Поэтому максимальная скорость передачи кадров составит в случае сети Modbus RTU при максимальной бодовой скорости 115,2 Кбод: (115200 бит/с)/ 2084 бит ~ 55,28 кадр/с. Пропускная способность равна: 55,28 кадр/с х 252 байта = 13,93 Кбайт/с.

Эффективность использования физической скорости передачи сети, в случае Modbus RTU равной 115,2 Кбод, по отношению только к полезным данным составит:

55,28 кадр /с х 2016 бит/ 115200 бит/с ~ 0,967 ~ 97 %.

3.2.2.2 При передаче кадров минимальной длины существенно возрастает скорость в кабеле, что означает всего лишь факт передачи большого числа коротких пакетов. В то же время пропускная способность и эффективность заметно (почти в два раза) ухудшаются из-за возрастания относительной доли служебной информации.

При типовых циклических запросах SCADA-системы о значении измеряемого параметра кадр содержит 164 бит (включая разделительную паузу), из которых 80 бит (10 байт) являются полезными данными. Максимальная скорость передачи кадров: (115200 бит/с)/ 164 бит « 702,44 кадр/с.

Пропускная способность в данном случае будет равна:

702,44 кадр/с х 10 байт ~ 7,02 Кбайт/с.

Эффективность использования физической скорости передачи сети: 702,44 кадр /с х 80 бит/ 115200 бит/с ~ 0,4878 = 48,78 %.

3.2.2.3 Следует отметить, что избыточность будет меньше при считывании данных с многоканальных устройств ввода данных, в которых данные измерений расположены подряд в регистровой карте.

Например, при считывании данных с 12-канального прибора цифрового контроля ПКЦ-12 (ЗАО «НЛП «Автоматика», г. Владимир), запрос, ответ и минимальная пауза между ними составляют 64,5 байт, а содержательной информации 54 байт (см. Рисунок 3.3). Снижение пропускной способности канала составляет около 16 %.

Запрос ведущего устройства:

адрес ведомого	номер функции	Адрес ст. байт	Адрес мл. байт	Количество регистров ст. байт	Количество регистров мл. байт	сис мл. байт	сис ст. байт
0x01	0x03	0x00	0x01	0x00	0x18	0x№4	ОхМчГ

Ответ ведомого устройства (ПКЦ-12):

адрес ведомого	номер функции	Количество байт	Данные 48 байт	сис мл. байт	СБ1С ст. байт
0x01	0x03	0x30	...	0x№4	ОхМчГ

Рисунок 3.3 - Цикл обмена информацией с многоканальным узлом сети МосШиэ ЯТи

3.2.3 Анализ влияния программных мер защиты в сети РгоАЬив БР защищённого Р-профиля

Сеть РгойЬиэ (БР и РА) кроме централизованного детерминированного доступа допускает возможность децентрализованного детерминированного доступа эстафетного типа. Ведущими могут быть до 32 узлов сети (из 128). Передача прав пользования магистралью производится по принципу эстафеты. Эстафетное кольцо представляет собой организованную цепь активных узлов с определенными заранее адресами. В этой цепи маркер (право доступа к среде) распространяется от одного ведущего к следующему в определенной последовательности увеличения адресов.

Одним из расширений стандарта РгойЬиБ является новое решение в области создания безопасных систем автоматизации на производстве (далее Б- профиль, или FailSafe-профиль). Впервые Р-профиль [35] был представлен на выставке в Ганновере в 1999 году. Основная задача этого расширения РгойЬиБ заключается в создании систем автоматизации, которые в своей эксплуатации безопасны как для людей, так и для машин. Эта новая технология включает такие компоненты, обеспечивающие безопасность труда, как аварийные кнопки останова, концевые выключатели, световые барьеры и лазерные системы контроля вместе с датчиками и исполнительными механизмами. Важным преимуществом использования Б-профиля является возможность объединения в единую сеть как устройств,

обеспечивающих безопасность, так и традиционных устройств, поддерживающих стандартный протокол РгоАЬив (БР или РА).

Рисунок 3.4 представляет в общем виде структуру БР-сообщения, включающего и защищенные данные, которые, в свою очередь, включены в состав общего блока данных. Всего из 244 байт полезных данных, которые могут быть переданы в одной ЭР-телеграмме, собственно защищенные данные могут составлять максимально 128 байт. Это ограничение связано с общим ограничением РгоАЬиэ ЭР, по которому за один цикл может быть прочитано/записано до 64 слов по инициативе ведущего абонента.

Обобщённый формат кадра в сети РгойЬиБ БР приведён на рисунке:

Sync Time	SD	LE	LEr	SD	DA	SA	FC	Data Unit	FCS	ED
33 бита	1 байт	1 байт	1 байт	1 байт	1 байт	1 байт	1 байт	до 244 байт	2 байта	1 байт

Sync Time - время синхронизации, SD - метка начала, LE - длина данных, LEr - повтор длины данных, DA - адрес приёмника, SA - адрес передатчика, FC - номер функции, Data Unit - данные, FCS - контрольная сумма, ED - метка конца сообщения.

Рисунок 3 4 - Кадр Profibus DP

Для считывания значения измеряемого параметра в формате Float 4, занимающем 4 байта, структура запроса входной информации и ответа в блоке данных (Data Unit) выглядят как показывает Рисунок 3.5:

Запрос ведущего устройства:

контрольный байт	последовательный счётчик	контрольная сумма 2 (CRC2)
1 байт	1 байт	2 байт

Ответ ведомого устройства:

защищённые данные	байт состояния	последовательный счётчик	контрольная сумма 2 (CRC2)
4 байта	1 байт	1 байт	2 байт

Рисунок 3.5 - Структура блоков данных в цикле обмена информацией с одноканальным узлом сети РгоШэш ЭР

Передача каждого байта данных требует дополнительно 1 стартового бита и 2 стоповых бит контроля (на чётность не проводится). Дополнительные биты

относятся к управляющим (служебным), они обеспечивают синхронизацию обмена байтами.

Необходимой информацией для исполнения команды считывания входных данных является «адрес приёмника», «номер функции» в запросе и собственно «защищённые данные» в ответе. Всего 6 байт. Запрос, ответ и минимальная пауза между ними составляют 36 байт. Очевидно, что введение защиты в форме избыточности кодирования, т.е. добавления двух полей «контрольная сумма», «количество байт данных», квитанций «адрес ведомого» и «номер функции», - приводит к снижению пропускной способности канала на 83 %:

$$100x\ (6 - 36)/36 = - 83{,}3\ \%.$$

Таким образом, дополнительная защита программными методами существенно снижает пропускную способность канала для характерных в сетях нижнего уровня АСУ ТП коротких сообщений.

3.3 Экспериментальная проверка защищённости телекоммуникаций нижнего уровня АСУ ТП.

Телекоммуникации нижнего уровня АСУ ТП в подавляющем большинстве случаев используют проводные линии связи. В лучшем случае — это экранированная витая пара.

Проникновение в сеть возможно при физическом подключении к линии связи. Это можно сделать в клеммных коробках разветвителей, контроллеров, датчиков, если доступ к ним недостаточно защищен.

Однако на практике чаще случаются ошибки монтажа, совпадения адресов, неправильная установка скорости обмена и т.п. Ошибки задерживают отладку АСУ ТП, особенно, если затруднено их обнаружение и локализация.

Автором была проверена реакция системы контроля и датчиков на включение второго ведущего в сеть МосИэш ЯТи. Для проверки автором разработана программа «МоёЬи8_Маз1ег», которая позволяет генерировать запросы, в том числе с ошибками, и получать статистическую информацию о событиях в сети.

Целью проведения эксперимента было определение возможности включения второго ведущего в централизованную детерминированную сеть МоёЬиБ ЯТи,

выявления последствий такого вмешательства для легального ведущего и для подчиненных узлов сети.

Рисунок 3.6 показывает зависимость процента обнаруженных ошибок обменов легального ведущего от скорости сети с четырьмя ведомыми при цикле опроса 1 с

.

30 25 **20** 15 10 5 0

Рисунок 3.6 - Зависимость процента обнаруженных ошибок обмена от скорости передачи

Генерация запросов нелегального ведущего производилась программой «МоёЬиз_Маз1ег» 1 раз в секунду независимо (асинхронно) от легального ведущего.

При включении алгоритма прослушивания сети и генерации посылок только после 10-миллисекундного «молчания». Программа «МоёЬиз_Маз1ег» обеспечила практически 100 % доступ к ведомым узлам сети, не нарушая циклы обмена легального ведущего. COM-порт легального ведущего получал дополнительные несанкционированные посылки. Но 8САОА-система никак на них не реагировала, то есть вмешательство не обнаруживала.

Адреса узлов в сети нелегальный ведущий может получить простым «прослушиванием» сети или сканированием. Скорость обмена может определить методом проб.

Из этого можно сделать следующие выводы:

1. Результаты эксперимента показали, что вмешательство нелегального ведущего физически возможно и не распознается легальным ведущим как вмешательство. Легальный ведущий воспринимает вмешательство нелегального ведущего как ошибку обмена только при наложении сигналов. Основное негативное воздействие вмешательства нелегального ведущего - ошибки обмена при наложении сигнала.

2. При низкой скорости обмена вмешательство нелегального ведущего в большей степени блокирует работу системы, которая констатирует ошибки обмена по сети.

3. При высокой скорости обмена нелегальный ведущий чаще успевает произвести обмен с ведомым узлом в промежутках между обменами легального ведущего. При этом легальный ведущий получает в буфер COM-порта сообщения, но не распознает их как вмешательство. А ведомые узлы исправно исполняют команды нелегального ведущего.

1,2	2,4	4,8	9,6	19,2	38,4	57,6	115,2
Кбит/с							

3.4 Разработка алгоритма доступа к узлам сети нижнего уровня АСУ ТП

Предложенный автором системный подход к построению СЗИ, предполагает кроме внешней защитной оболочки, организованной БСАБА- системой и операционной системой, создавать и использовать встроенные механизмами защиты в программных и технических компонентах нижнего уровня АСУ ТП.

Защита интеллектуальных датчиков, исполнительных механизмов, приборов и контроллеров как со стороны встроенного пульта управления, так и со стороны локальной сети представляет из себя механизм цифрового или процедурного пароля. Т.е. доступ к изменению (записи) параметров устройства может быть открыт и закрыт нажатием определённой последовательности кнопок пульта или подачей специальных команд по сети.

Анализ защищённости интеллектуальных сетевых устройств нижнего уровня АСУ ТП показал, что тенденция разработки устройств с максимальной гибкостью, программируемостью приводит к неоправданному повышению риска НСД и

увеличивает число возможных ошибок обслуживающего персонала. Некоторые характерные результаты этого анализа, проведённого автором среди множества отечественных и зарубежных интеллектуальных устройств ввода-вывода [36-61] сведены в Таблице 3.2.

Таблица 3.2 - Защита доступа к сетевым устройствам АСУ ТП Устройство и производитель	Сеть (интерфейс)	Открытие доступа | Закрытие доступа	
Комплекс ТЕКОНИК® (10 сетевых модулей). ЗАО «ТеконГруп» (Россия)	T4000 (RS-485)	Замыкание перемычки WWZ\ на приборе. По сети - командой «Перейти в режим «конфигурировани я» ($AACPO)	Выключение питания прибора. По сети - командой «Перезапуск датчика» ($AARST)
Комплекс «ДЕКОНТ» (около 30 сетевых модулей). Компания ДЭП (Россия)	CAN, Ethernet (RS-232, RS-485, USB, SSI)	Модули не имеют встроенного пульта, полностью управляются по сети или с переносного пульта. Защита паролями на уровне программ «Конфигуратор», «Клиент-Сервер».	
Датчик «Rosemount 3051 >>. Emerson Process Management (США)	Foundation fieldbus	Снять перемычку защиты от записи на приборе	Установить перемычку защиты от записи на приборе
Датчик «Cerbar S». Endress+Hauser (Германия)	Foundation fieldbus	Одновременное нажатие кнопок «+8» и «-г» на приборе. По сети - командой с кодом 130	Одновременное нажатие кнопок «+Z» и «-8» на приборе. По сети - командой с кодом, не равным 130
Приборы «ПРОМА-ИДМ», «ПРОМА-ИТМ». ООО «ПРОМА» (Россия)	Modbus RTU (RS-485)	Одновременное нажатие кнопок «|» и «1» на приборе	Одновременное нажатие кнопок «|» и «|» на приборе
		Доступ по сети свободный	
Прибор Ф1791. Завод «ВИБРАТОР» (Россия)	Modbus RTU (RS-485)	Пароль из 3 цифр с пульта прибора(по сети только чтение)	Нажатие кнопки «Вход»
Датчики «Метран-100». ПГ «Метран» (Россия)	ICP, Modbus (RS-485)	Доступ по сети свободный. 1 Защита паролями на уровне конфигурационной программы 1СР- МА8ТЕ^ Modbus-MASTER **или** ЗСАВА-системы	
1 Модули ввода-вывода серии «NL-M». | НИЛ АП (Россия)	ASCII, Modbus (RS-485)	Доступ по сети свободный через ОРС- сервер ^орс от любой ЗСАОА-системы	

Таким образом, потенциальная опасность НСД существует, несмотря на наличие паролей и процедур начала и окончания настройки, т.к. высока вероятность того, например, что оператор забудет закрыть процедуру настройки. А для узлов, свободно доступных по сети или открываемых по сети, опасность НСД наиболее высока.

Не надо забывать и о том, что легальному пользователю защита не должна добавлять чрезмерных неудобств.

Автор предлагает следующие алгоритмы доступа к узлам сети со стороны пульта (Рисунок 3.7) и со стороны сети (Рисунок 3.8), отличающиеся от существующих тем, что оптимально сочетают ряд методов защиты от НСД с предложением доступ к настройкам по сети только закрывать.

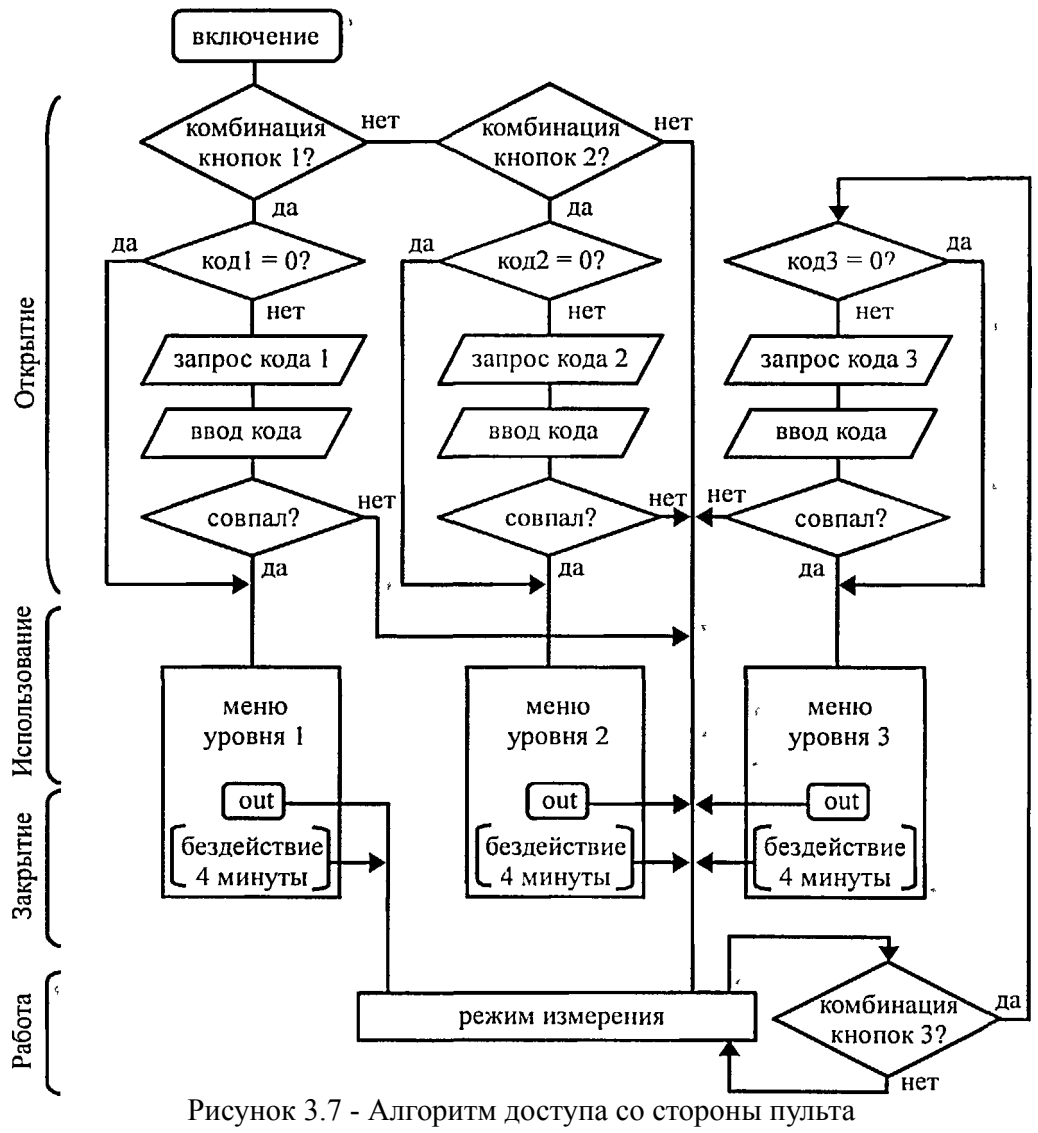


Рисунок 3.7 - Алгоритм доступа со стороны пульта

В предложенном алгоритме работы пульта открытие доступа для настройки (записи) производится нажатием комбинации кнопок и вводом цифрового кода (пароля). Причём открытие доступа возможно только с пульта прибора, а закрытие доступа либо с пульта (выход «out» из меню), либо командой по сети (Рисунок 3.8), либо автоматически по истечении 4 минут после последнего нажатия кнопок пульта прибора. Не получив физического доступа к пульту каждого прибора нельзя их перенастроить. Доступ к особо ответственным настройкам (метрологические характеристики, коды доступа, восстановление заводских настроек) следует предоставлять только при включении питания узла, что дополнительно усложняет доступ и позволяет легко обнаружить его.

Эти неудобства не чрезмерны, если учесть, что такие настройки производятся только в период пуско-наладочных или ремонтных работ. Причём открытие доступа без пароля (код = 0) и открытие доступа по сети отменяют автоматическое закрытие доступа по истечении 4 минут бездействия пульта, т.е. настройка по сети возможна вплоть до её запрета командой по сети.

На Рисунке 3.8 показан участок алгоритма обработки команд записи в ведомом узле, ответственный за доступ к записи настроечных параметров. Он отделяет управление регистром маски доступа (блок 1), разрешая только закрытие доступа (блоки 7, 8); увязывает разрешение записи с маской доступа (блоки 2, 3) и не проводит запись, если новые данные совпадают с уже имеющимися (блок 4) для сбережения времени и ресурса flash-памяти.

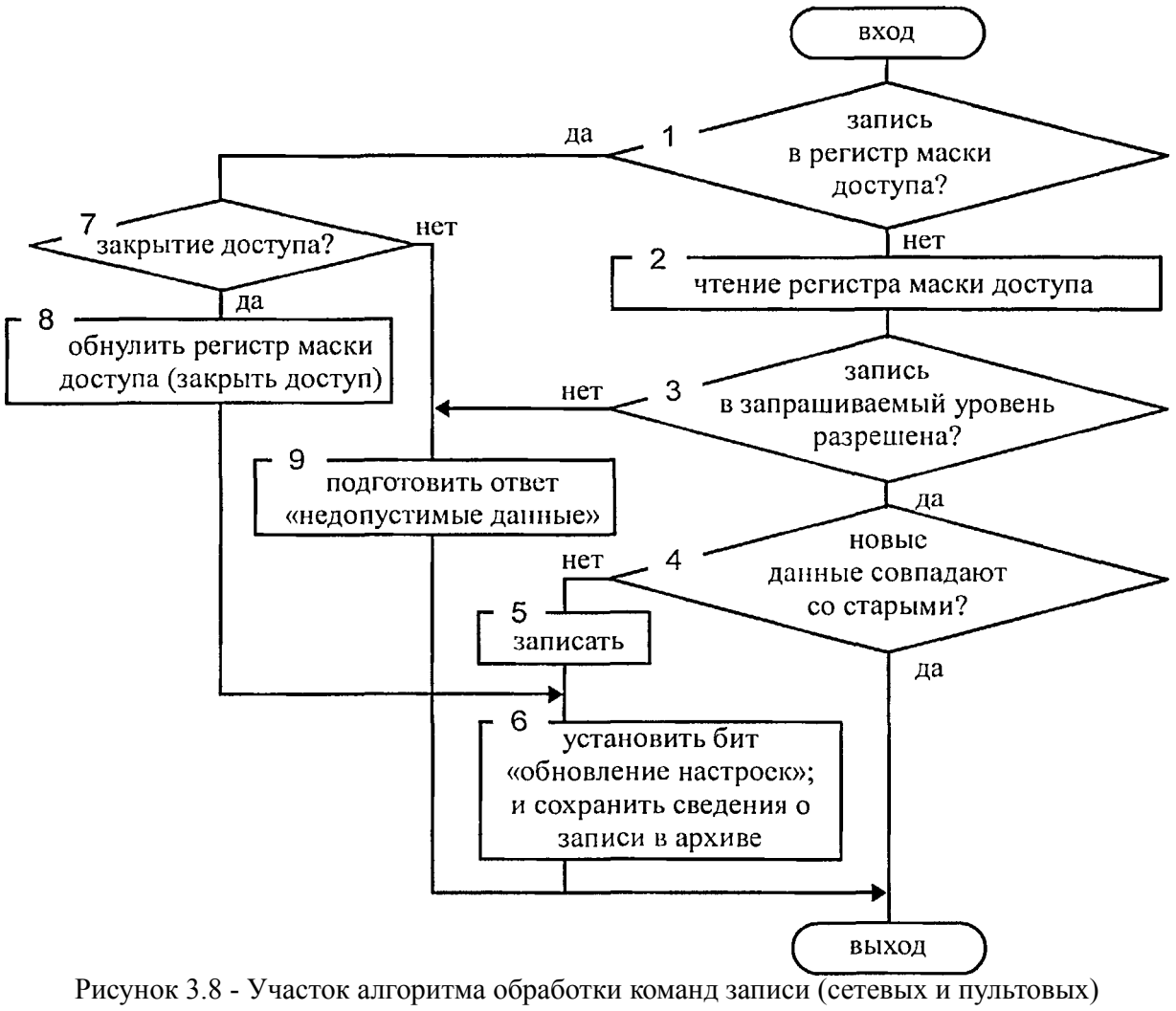


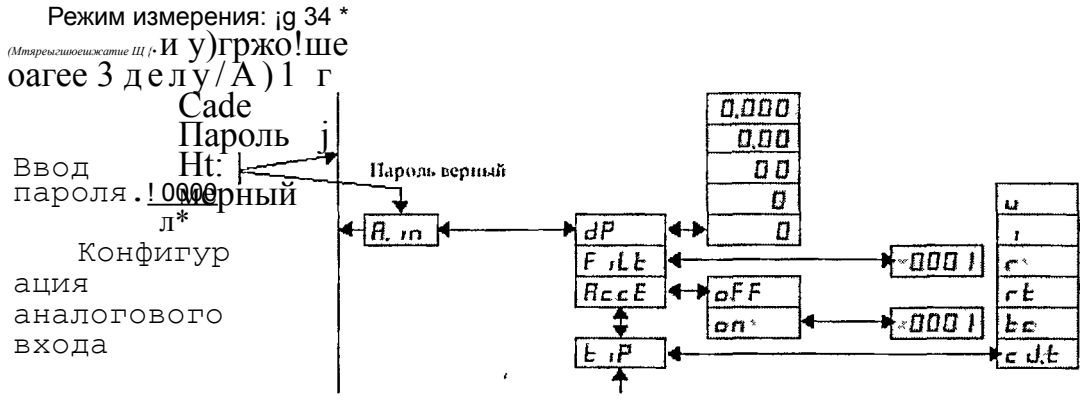
Рисунок 3.8 - Участок алгоритма обработки команд записи (сетевых и пультовых)

Кроме того, автор предлагает любые изменения настроек прибора отражать в его архиве событий записью логина, пароля и времени, а также в его регистре диагностики установкой бита обновления настроек. «Ведущий» сети должен прочитать регистр диагностики «ведомого», проверить изменения и сбросить бит обновления настроек. Регулярный контроль этого бита легко осуществить, если «ведомый» копирует его в байт статуса в ответе «ведущему». БСАБА-системы обычно обрабатывают байт статуса в ответах, и это не является дополнительной нагрузкой. Такой алгоритм существенно снижает вероятность НСД и обеспечивает быстрое обнаружение вторжений в настройки, не усложняя работу с узлом сети в процессе эксплуатации.

Предложенный автором алгоритм реализован в интеллектуальных датчиках ПД-1ЦМ [62, 63], ИТ-1ЦМ [64, 65] и вторичных приборах ПКД-1115

[66-68], ПКЦ-1111 [69-71] производства ЗАО «НПП «Автоматика» (г. Владимир). Пример конкретной реализации алгоритма в меню прибора ПКД- 1115 [67]

иллюстрирует Рисунок 3.9 (показан начальный и конечный участки одной из пяти ветвей управления с пульта). Здесь использован процедурный и цифровой пароли доступа в меню, индивидуальное открытие и закрытие доступа по сети (подменю «гё» —> «гб.Еп») к настройкам аналогового входа «Алп», аналогового выхода «А.оиЬ>, дискретных выходов «с!.оиЪ>, параметров интерфейса «гЭ» и сервисных функций «г8ъ>.



fciSJ
5 7.5
I a J
9.6

Конфигурация интерфейса

EUEn *DO IS*

aaia

r 5 j4->bffud

Я5П

fl.oufe

d.oufc

Ion

on «

Сервис

(воесыпоплсгшс гаюдскнх настроек и смена кодд доступа ровню .\'»1)

Рисунок 3.9 - Меню конфигурации ПКД-1115

Автором проведены сравнительные испытания датчиков ПД-1ЦМ и приборов ПКД-1115 с датчиками и приборами аналогичных изделий в сети Modbus RTU SCADA-системы «MySCADA» (разработана ЗАО «НЛП «Автоматика») в режиме имитации НСД с использованием авторской программы Modbus_Master.

Для сравнительной оценки защищённости узлов сети от НСД автор предлагает использовать отношение сумм остаточных рисков: $S*2i = £ Risk_2 \ / £ Risk_u$,

где $Riski — PiL,Ri$ - оценка математического ожидания потерь (риск), Pi - вероятность появления i-й угрозы,

$L\$ - величина ущерба при удачном осуществлении i-й угрозы в отношении защищаемых объектов (уровень серьезности угрозы),

R_i - вероятность уязвимости, т.е. преодоления механизма защиты. Сравнивая два узла сети №1 и №2, выполняющих одинаковые или близкие функции, можно свести отношение рисков к отношению вероятностей уязвимости (преодоления барьера защиты):

Ям = 1Д2|/1Дц, (3.4.1)

т.к. в этом случае для всех I : $P_n — P\ \ L_2\ = L_n$

В качестве оценки вероятности преодоления механизма защиты R_i использована относительная частота преодоления механизма защиты по экспериментальным данным имитации НСД (величина, обратно пропорциональная количеству попыток до получения доступа).

Защищенность узлов определяется как величина, обратная их «уязвимости» или риску, поэтому Sz\<l означает меньшую защищённость узла №1.

Таблица 3.3, Таблица 3.4, Таблица 3.5 и Рисунок ЗЛО, Рисунок 3.11, Рисунок 3.12 содержат относительные частоты появления обнаруженных и не обнаруженных мастером сети (MySCADA) вторжений в настройки узлов сети со стороны пульта и по сети нелегальным мастером (Modbus_Master). Таблица 3.4 получена при асинхронной работе нелегального мастера (Modbus_Master), когда возможно наложение запросов нелегального мастера на обмены легального мастера. Таблица 3,5 получена при синхронизации запросов Мо<ЗЬиз_Ма51ег с паузами в обменах легального мастера сети МуБ- САЛЭА.

Таблица 3.3 - Относительные частоты НСД с пульта НСД **с пульта**	**ПД**-1ЦМ	пкд- **1115**	**Метран-** **100**	**Ф1791**	1ЧЬ-8А1"	ПРОМА -ИДМ
обнаруженный	0,001	0,001	0,005	0,008	0	0
не обнаруженный	0	0	0	0,017	0	0,50

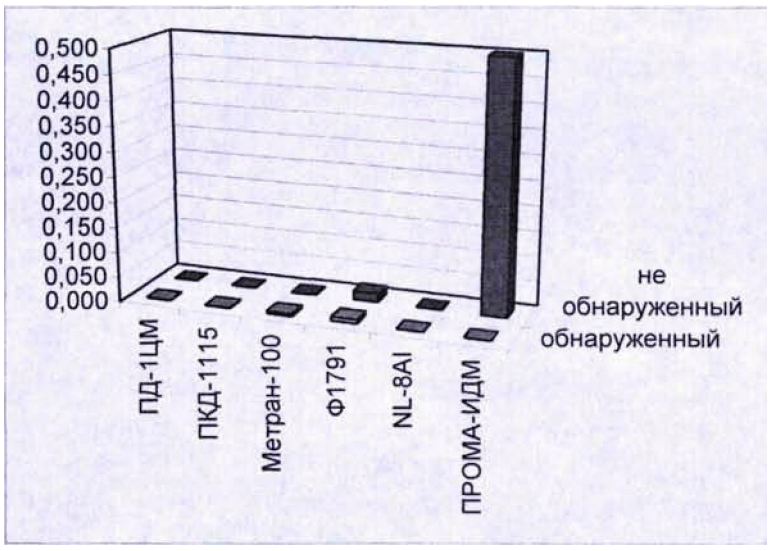


Рисунок ЗЛО - Относительные частоты появления обнаруженного и не обнаруженного НСД с пульта

Таблица 3.4 - Относительные частоты асинхронного НСД по сети **НСД по сети**	пд- **1ЦМ**[21]	пкд- **1115**[2)]	**Метран-** 100[2)]	**Ф1791**[2']	**1ЧЬ-8А1**[п]	ПРОМА -идм[3)]
обнаруженный	0,0005	0,0005	0,003	0,008	0,30	0,35
не обнаруженный	0	0	0	0.025	0,20	0,65

асинхронного НСД через сеть

Таблица 3.5 -	ПД-1ЦМ[21]	ПКД-П15[2)]	Метран-100[2)]	Ф1791[4]	N1^-8 А1[1)]	ПРОМА -ИДМ[3)]
Относительные частоты синхронного НСД по сети						

НСД по сети						т
обнаруженный	0,001	0,001	0,01	0,01	0,01	0
не обнаруженный	0	0	0	0,08	0,50	1

Примечания:

" В датчике не обнаруженный «N1.-8A1» для обнаруженный доступа по сети

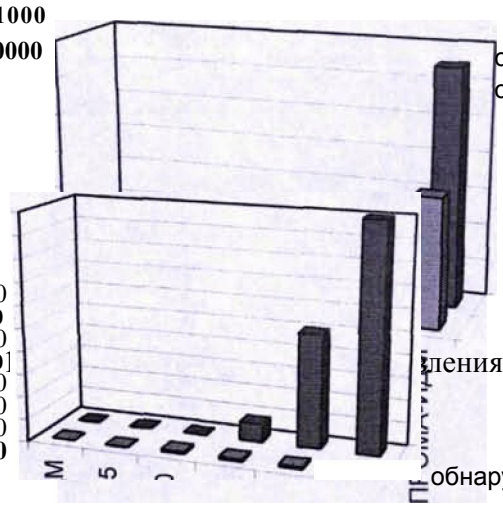


Рисунок 3.11 - ления обнаруженного и не обнаруженного

не устанавливается обнаруженны перемычка. [2} обнаруженны открывается с й защиты доступа

Доступ пульта прибора. [3] Прибор не имеет по сети.

Рисунок 3.12 - Относительные частоты появления обнаруженного и не обнаруженного синхронного НСД через сеть

Результаты сравнительной оценки защищённости по формуле (3.4.1) приборов ПКД-1115 с аналогами представлены в Таблица 3.6 и на Рисунок 3.13.

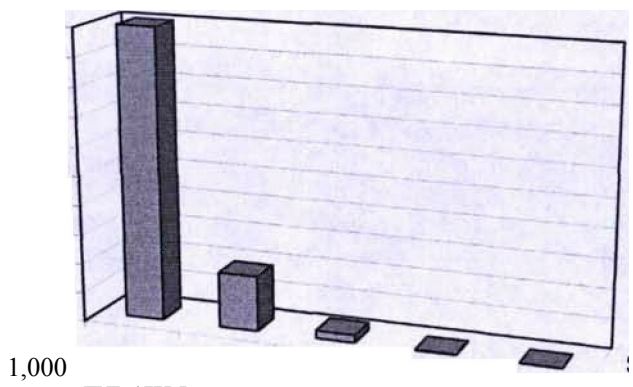


Рисунок 3.13 - Сравнительная оценка защищённости

Высокая защищённость ПД-1ЦМ и ПКД-1115 получена за счёт использования бита обновления настроек и передачи его в байте статуса прибора в каждом ответе, а также тем, что открыть доступ к настройкам из сети можно только с помощью пульта (специальной процедурой с отключением питания и вводом пароля). Прибор «Ф1791» имеет пароль всего из трёх цифр (у ПКД, ПД и Метрана - 4 цифры). Приборы «ЫЬ-8А1» и «ПРОМА-ИДМ» не имеют бита обновления настроек и регистра диагностики; доступ к ним по сети не защищён мерами самого прибора. НСД в приборы «ЫЬ-8А1» и «ПРОМА-ИДМ» фактически обнаруживался только как сбой обмена, поэтому при синхронизации запросов МосШи5_Маз1ег с паузами в обменах легального мастера относительная частота не обнаруженного НСД сравнялась с 1.

Таблица 3,6 - Сравнительная оценка защищённости

3.5 АСУ ТП производства бумвинила «ПХВ-1» 3.5.1 Область применения АСУ ТП

В данной главе анализируются технические особенности проектирования распределенных автоматизированных систем управления технологическими процессами в химической промышленности на примере АСУ ТП производства бумвинила, внедренную на предприятии ООО «ПСВ-Холдинг».

Здесь наиболее ярко отражаются требования к АСУ ТП по информационной безопасности, надёжности, устойчивости к воздействию климатических факторов и другим характеристикам. Поэтому автоматизация этой важной и ответственной отрасли должна выполняться в соответствии с жесткими требованиями по безопасности [72].

Автор анализировал существующие механизмы защиты информации в АСУТП «ПХВ-1», принимал участие во внедрении данной АСУ ТП. После проведенного анализа данной АСУ ТП, автор выработал рекомендации по обеспечению информационной безопасности.

3.5.2 Архитектура автоматизированных систем

Архитектура АСУ ТП весьма существенно влияет на состав программно-аппаратных средств. АСУ ТП подразделяются на два основных типа:

- централизованные АСУ ТП;
- распределенные АСУ ТП.

Централизованные АСУ ТП являются комплексами, как правило, занимающими единое ограниченное производственное пространство с централизованной подсистемой обеспечения электропитанием и магистралями для обмена информационными потоками.

Распределенные АСУ ТП строятся на базе объектов, расположенных на различных, отчасти далеко расположенных, закрытых и открытых площадках. Именно эта особенность накладывает определенные структурные требования при проектировании распределенных АСУ ТП.

АСУ ТП производства бумвинила можно отнести к классу распределенных АСУ ТП, так как производственные зоны разнесены на существенной территории и

расположены в нескольких зданиях, операторские станции расположены в отдельно стоящем здании на территории предприятия.

Диспетчеризация всего производственного комплекса осуществляется через глобальную сеть. Головной офис компании находится в другом городе, задания на производственный участок передаются с помощью сети Интернет. Также через Интернет осуществляется предоставление отчетности в головной офис. (Это уже АСУ предприятия).

3.5.3 Технические требования к распределенным АСУ ТП Основными техническими требованиями при проектировании распределенных АСУ ТП являются:

- обеспечение широкого температурного диапазона работы технических средств локальных систем автоматического управления (САУ);
- распределенная система электропитания;
- обеспечение надежного контура заземлений на каждой отдельной площадке объекта автоматизации;
- защита контрольно-измерительных и информационных каналов от внешних воздействий, а также усиление передаваемых сигналов;
- выбор оптимального, с точки зрения эффективности, надежности и взаимозаменяемости составных частей, удовлетворяющего международным стандартам контроллерного оборудования;
- выбор оптимального, с точки зрения пылевлагонепроницаемости, а также защиты от электромагнитного излучения, коррозии и др. факторов, удовлетворяющего международным стандартам конструктива шкафа цехового контроллера, шкафов автоматики локальных САУ и автоматизированного рабочего места системного инженера (АРМ СИ);
- обеспечение высоконадежных каналов обмена технологической информацией между отдельными автоматизированными объектами и централизованной системой управления и контроля;
- резервирование основной аппаратуры контроля и управления, а также наиболее важных каналов передачи информации;

• обеспечение аппаратного и программного аварийного останова технологического комплекса при аварийных ситуациях;

• обеспечение высокоэффективного человеко-машинного интерфейса в системе визуализации и мониторинга;

• обеспечение обмена данными по информационным каналам в реальном масштабе времени;

• эффективная, с точки зрения скорости обнаружения неисправности, и надежная диагностика программно-аппаратных средств;

• обеспечение обслуживающего персонала качественной эксплуатационной документацией, а также инструментом для монтажа и диагностики.

В основе распределенной АСУ ТП производства бумвинила лежит программно-технический комплекс (ПТК) «ПХВ-1» (Рисунок 3.14), который в основном удовлетворяет требованиям, изложенным выше.

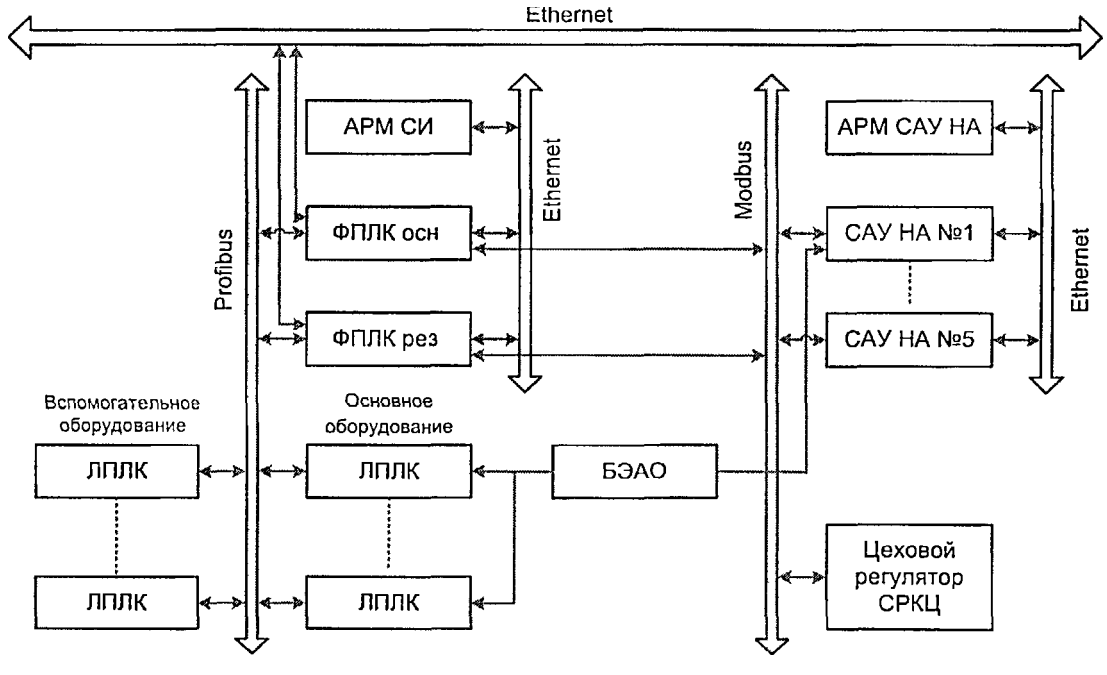


Рисунок 3.14 - Структурная схема ПТК «ПХВ-1»

БЭАО - блок экстренного аварийного останова; АРМ СИ - автоматизированное рабочее место сменного инженера; АРМ САУ НА - автоматизированное рабочее место системы автоматического управления напыляющими агрегатами;

ФПЛК — фронтальный программируемый логический контроллер;

ЛПЛК — локальный программируемый логический контроллер.

ПТК «ПХВ-1» рассчитан на эксплуатацию в закрытых отапливаемых или не отапливаемых помещениях. ПТК «ПХВ-1» может работать в непрерывном режиме круглосуточно.

Электропитание осуществляется от сети переменного тока 1 категории с резервированием источниками бесперебойного питания.

Защита цепей питания, измерительных и информационных каналов от электромагнитных помех, перенапряжений, вторичных проявлений грозовых токов и возникновение искры во взрывоопасной зоне осуществляется защитными барьерами искробезопасности. Во взрывоопасной зоне применяются датчики во взрывобезопасном исполнении (Exd).

Используются шкафы фирмы RITTAL со степенью защиты IP54.

Система безопасности рабочего персонала и эксплуатационного оборудования ПТК «ПХВ-1» базируется на применении блока экстренного аварийного останова (БЭАО), который является распределенным аппаратным устройством.

Более подробные технические характеристики ПТК «ПХВ-1» приведены в Приложении 6.

3.5.4 Контроллерное оборудование

Выбор состава контроллерного оборудования является наиболее важным в архитектуре распределенного АСУ ТП. Оптимальным решением принято применение промышленных контроллеров на базе открытых систем, таких как VME9000, IUC9000 и SMART производства фирмы «PEP Modular Computers». Данные контроллеры по своей архитектуре и технологии соответствуют известным международным стандартам и имеют следующие основные характеристики:

- системная шина VME для фронтальных котроллеров цехового применения;
- локальная шина для локальных контроллеров типа IUC9000 и SMART;

- встроенная операционная система реального времени OS9, предназначенная для промышленных контроллеров;
- мезонинная технология с ориентацией на гибкую конфигурацию;
- прикладное обеспечение на базе открытых инструментальных систем типа ISaGRAF (стандарт IEC6131-3);
- стандартный сетевой интерфейс типа Ehternet, Profibus, Modbus;
- широкий выбор взаимозаменяемых модулей УСО;
- конструктив типа «Евромеханика», обеспечивающий удобство монтажа, механическую совместимость, высокую помехозащищенность и сертифицированную защиту от механических и климатических воздействий.

3.5.5 Интерфейсы

ПТК «ПХВ-1» использует внутренние и внешние физические интерфейсы для обмена информационными данными. Внутренний интерфейс обеспечивает обмен структурами данных между цеховыми и локальными контроллерами; внешние интерфейсы обмен данными между цеховыми контроллерами и ДП (диспетчерский пульт АСУ ТП), а также между локальными контроллерами и объектами автоматизации.

При передаче данных применяется как магистральный, так и радиальный физический тип интерфейса:

- ETHERNET внутренний, внешний магистральный;
- PROFIBUS внутренний магистральный/радиальный;
- RS-485/232 внешний радиальный.

Для передачи данных на короткие расстояния (до 100 метров) применяется интерфейс Ethernet/Profibus с витой парой.

Физическая среда передачи данных интерфейса PROFIBUS соответствует стандарту PROFIBUS (DIN 19245).

Физическая среда передачи данных интерфейса RS-485 соответствует стандарту EIA RS-485.

Физическая среда передачи данных интерфейса ETHERNET соответствует стандарту IEEE 802.3.

3.5.6 Резервирование

Для увеличения надежности автоматизированной системы применено резервирование. Существуют разные подходы к реализации стратегии резервирования. Многое сводится к выбору между стоимостью и надежностью оборудования. Оптимальных решений, как правило, нет, однако есть базовые принципы, которые следует соблюдать при проектировании распределенных АСУ ТП, а именно:

- резервирование цеховых (фронтальных) контроллеров;
- распределение функций в многопроцессорной системе фронтальных контроллеров;
- резервирование информационной магистрали или локальных контроллеров наиболее ответственных объектов;
- резервирование цепей аварийного останова системы;
- резервирование контрольно-измерительных каналов (по необходимости).

Исходя из этого, в ПТК «ПХВ-1» резервируются следующие элементы:

- цеховой (фронтальный) контроллер;
- проводной канал РКОРЮиЭ локального контроллера узла подключения;
- коммутационные цепи аварийного останова.

Кроме того, производится распределение функций в двухпроцессорной системе фронтальных контроллеров.

3.5.7 Информационное обеспечение

Информационное обеспечение базового программного комплекса ПТК «ПХВ-1» состоит из данных, размещенных на трех уровнях комплекса:

- АРМ СИ цеха;
- Цеховой (фронтальный) ПЛК (ФПЛК);
- Локальные ПЛК (ЛПЛК), установленные на объектах.

Принципы организации и идентификации данных основываются на особенностях многоуровневой структуры ПТК «ПХВ-1». Также учитывается,

что ПТК является составной частью системы АСУ ТП и может иметь интерфейсы со смежными системами.

На каждом уровне базового программного комплекса ПТК обеспечена защита данных от разрушений при авариях и сбоях электропитания. На уровне АРМ СИ цеха данные сохраняются в файлах журналов. На уровне фронтального ПЛК (ФПЛК) база значений переменных и структуры, описывающие конфигурацию подсистемы, сохраняются в статической памяти. Статическая память ФПЛК не разрушается при авариях и сбоях электропитания.

Основу информационного обеспечения АРМ СИ цеха составляет база данных, разработанная и функционирующая в среде SCADA-системы INTOUCH (компании Wonderware). Формирование базы данных и обеспечение визуализации данных на видеокадрах осуществляется в интерактивном режиме среды INTOUCH.

В состав программного обеспечения АРМ СИ входит специальное приложение OPC-сервер, работающее в среде Windows NT совместно с пакетом INTOUCH.

Информационный обмен обеспечивает выполнение следующих функций:

- сбор данных от ЛПЛК в ФПЛК не реже, чем 1 раз в 0,5 с;
- получение от ЛПЛК в ФПЛК изменений приоритетных (инициативных) данных не реже, чем через 0,3 с;
- выдача на ЛПЛК от ФПЛК управляющих воздействий (время прохождения одного управляющего воздействия должно составлять не более 1 с);
- получение от ЛПЛК в ФПЛК диагностической информации;
- выдачу на ЛПЛК от ФПЛК команд синхронизации времени;
- выдачу на ЛПЛК от ФПЛК информации, управляющей работой ЛПЛК.
- сбор на ФПЛК от ЛПЛК информации по технологическому процессу. ФПЛК опрашивает ЛПЛК с помощью циклических запросов;

• передача от ЛПЛК в адрес ФПЛК измененных приоритетных сигналов (по инициативе ЛПЛК);

• передача команд по управлению процессом (специфические команды по управлению оборудованием) от ФПЛК в ЛПЛК.

Информационный обмен между цеховым и локальными контроллерами обеспечивается магистралью PROFIBUS на основе витой пары (до 115 Кбод/с).

Информационный обмен между цеховым контроллером и АРМ СИ обеспечивается магистралью Ethernet с известными физическими характеристиками (экранированная витая пара).

Информационный обмен между цеховым контроллером и смежными САУ обеспечивается магистральным интерфейсом RS-485 по протоколу Modbus. Модули УСО, подключаемые к каналу RS-485 с гальванической развязкой, усиливают помехозащищенность канала данных.

3.5.8 Диагностика ПТК

Диагностика ПТК обеспечивается на всех трех уровнях.

На уровне АРМа диагностируется состояние контроллеров (до отдельного модуля УСО) и магистралей обмена данными. Кроме того, в журнале событий фиксируется состояние аварийного сигнала.

На уровне цехового контроллера выполняется контроль связи Ethernet между цеховым контроллером и АРМ, контроль связи между цеховым контроллером и САУ НА (системы автоматического управления напыляющим агрегатом) каждого агрегата, диагностика состояния узлов в сети PROFIBUS.

На уровне локального контроллера обеспечивается контроль работы узла (мастера) в сети PROFIBUS в задаче ISaGRAF, контроль входов модулей УСО, контроль входных сигналов (выход за пределы диапазона).

Для обслуживающего персонала на передних панелях процессорных модулей и блоков питания имеется световая индикация питания (+5V), состояния PROFIBUS (Tx), состояние Ethernet (Col), возможна программная индикация для пользователя (8 индикаторов). На кросс-модулях имеется индикация каждого дискретного канала и питания кросса. Каждый ИП имеет индикацию питания. Состояние ИП, модулей

оптических преобразователей дверных концевых выключателей контролируется системой диагностики ПТК.

3.6 Методы отладки АСУ ТП «ПХВ-1»

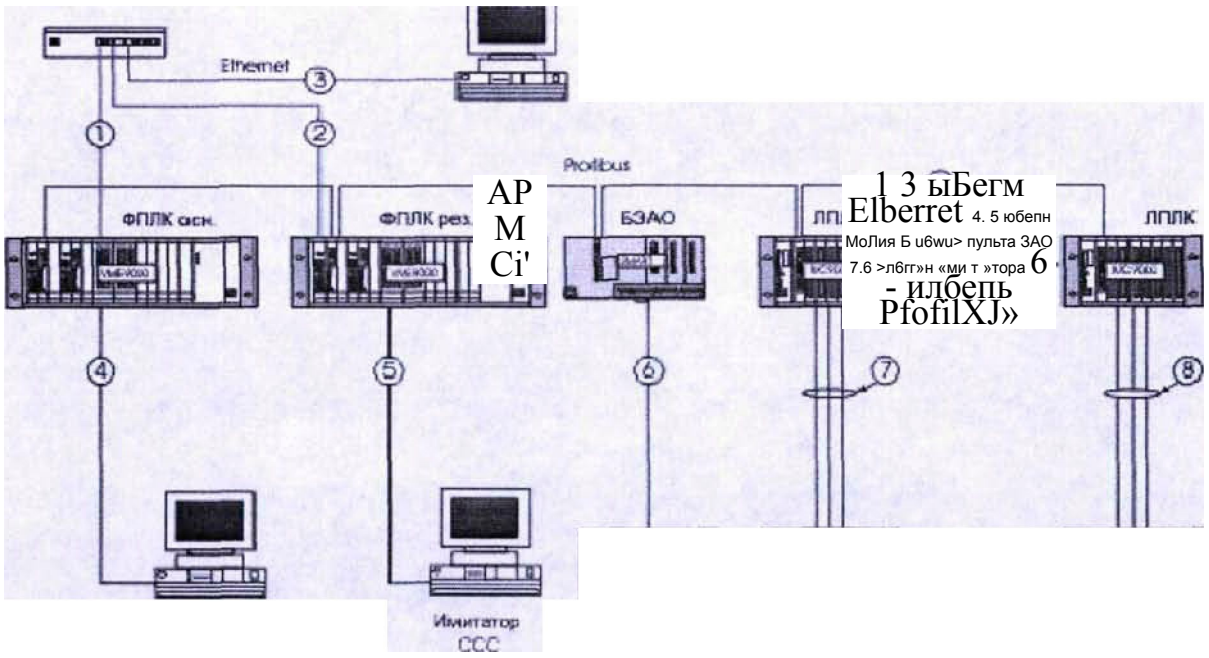
В настоящее время существует множество методов отладки и диагностирования АСУ ТП. Все они подразделяются на два основных типа:

- статический;
- динамический.

Статический метод характеризуется выработкой определенных требований к сервисной аппаратуре и стендам, которые включают входной контроль источников питания, модулей цифрового и аналогового ввода-вывода, а также подбор аппаратуры для контроля и испытаний. Кроме того, разрабатываются информационно-измерительные системы для автоматизации испытаний (Рисунок 3.15).

Динамический метод включает комплексную отладку системы и отладку алгоритмов работы системы. Динамический метод, с точки зрения метрологии, не является точностным методом, однако он может обеспечивать полную нагруженность системы переменными, работающими в реальном масштабе времени, задавать сложные специализированные алгоритмы и таким образом максимально имитировать работу системы, приближая получение реальных рабочих характеристик. Именно поэтому в данной главе уделено наибольшее внимание отладке АСУ ТП в динамическом режиме.

Для контроля работоспособности аппаратуры и комплексной отладки программно-технического комплекса «ПХВ-1» в рамках разработки проекта системы автоматизации производства бумвинила «ПХВ-1» были использованы оба метода отладки и диагностирования комплекса АСУ ТП.



АР
М
Ci'

1 3 ыБегм
Elberret 4. 5 юбепн
МоЛия Б u6wu> пульта ЗАО
7.6 >лбгг»н «ми т »тора 6
- илбепь
PfofilXJ»

Имитатор обьек-та
в

Иикгат
ор
СС

Имит
атор
объек
та

ФП С - фвоигагк.1!ЫМ
nротраммируемый контроллер

ЛПШ - гижжльнь« гчиграмныруиныи
кок t роллер

АРМ СИ - оя памяти »роя иное рэйоие
песта сиетс-июш MKttntcpa.

Пулы
БЭАО

Рисунок 3 . 1 5 - Схема соединений отладочного комплекса «ПХВ-1»

На Рисуике 3.16 и Рисунке 3.17 представлены схемы статической и динамической отладки входных-выходных сигналов телесигнализации, телеизмерений и управления. (ТС, ТИ, ТУ).

Note hock

И
Л
2
4
8

Rs-гзг

X

F DIN FDOUT FREL FADC FDAC

ИСИМТВ
1НП1+.ЫИ

Kaiu. iHpai op 81-13

Магаз ин со прошила ' нии

c ne na

tEft ffttif »<№ ilrfi 'M'l «u» Л 1.1,0».! 4LÏU1, nuKmim Wl

Рисунок 3.16 - Схема статической отладки входных-выходных сигналов ТС, ТИ и ТУ

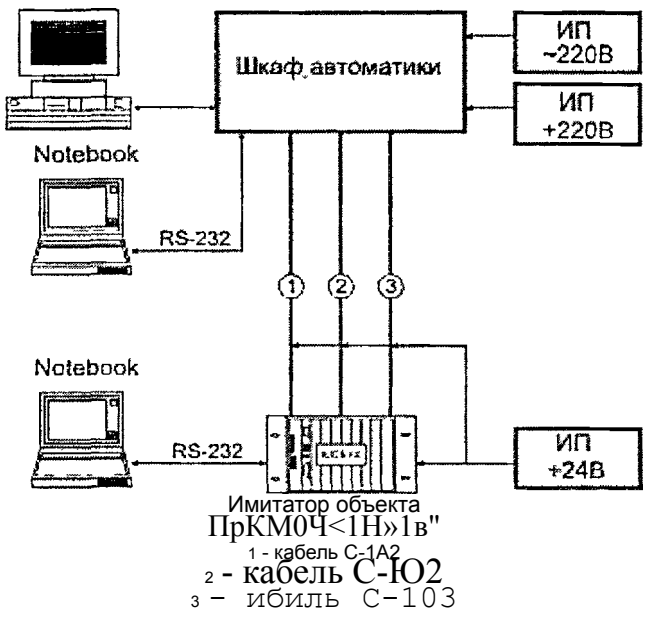


Рисунок 3.17 - Схема динамической отладки входных-выходных сигналов ТС, ТИ и ТУ

3.6.1 Отладка алгоритмов работы системы

Для отладки отдельных алгоритмов работы программного обеспечения на входы модулей ввода подаются сигналы, имитирующие поведение объекта. Преимуществом рекомендованного автором метода моделирования НСД и мер защиты от него, а также других нештатных ситуаций, с помощью контроллеров-имитаторов и задач-имитаторов из штатного ПТК, является простота подготовительных операций. Подготовительные операции заключаются в изготовлении кабелей-переходников для передачи аналоговых сигналов от ЦАП к АЦП и от модулей цифрового вывода к модулям цифрового ввода (с подключением внешнего источника питания). На Рисунке 3.18 дана блок- схема специализированного алгоритма управления краном, реализованная при отладке комплекса «ПХВ-1» с помощью имитатора объекта.

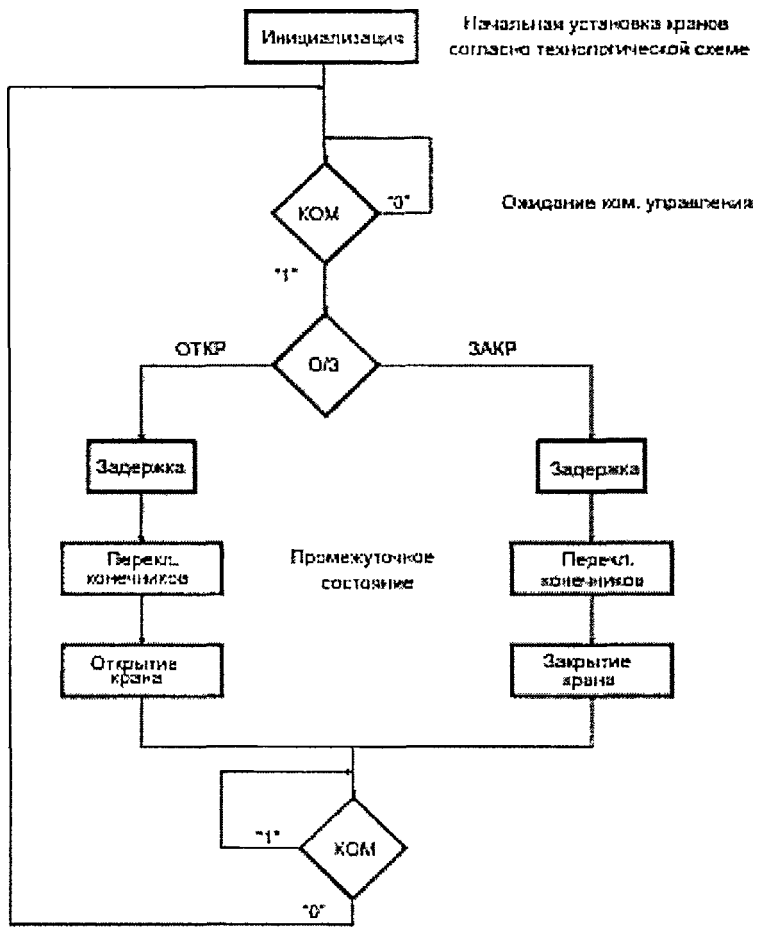


Рисунок 3.18 - Блок-схема алгоритма управления краном **3.6.2 Имитаторы**

Для комплексной отладки системы необходимо иметь ряд аппаратных и программных имитаторов объектов. Имитатор объекта комплекса в составе комплекса «ПХВ-1» (Рисунок 3.14) является программно-аппаратным средством диагностики и отладки контроллеров РЕР типа IUC, VME, SMART, а также шкафов автоматики на базе данных контроллеров.

Имитатор выполняет следующие функции:

- контроль дискретных выходных сигналов;
- формирование дискретных входных сигналов;
- формирование циклических аналоговых сигналов;
- формирование пошагового режима аналоговых сигналов;
- выполнение алгоритма управления кранами;
- выполнение специализированных алгоритмов для отладки объектов.

Имитатор имеет информационную емкость по параметрам:

- количество каналов дискретных входов (ТС) — 40;

- количество каналов дискретных выходов (ТУ) — 32;
- количество каналов аналоговых выходов (ТИ) — 16.

Имитатор может работать в следующих режимах:

- диагностика модулей;
- контрольно-измерительный;
- специализированные алгоритмы.

Режим диагностики используется при проверке модулей УСО.

Контрольно-измерительный режим применяется для отладки модулей УСО в составе контроллеров РЕР или контрольно-измерительных каналов (КИК) в составе шкафа автоматики на базе контроллеров УСО. В данном режиме возможно формирование как статических, так и динамических аналоговых и дискретных сигналов в циклическом и пошаговом режиме, а также контроль и индикация входных дискретных сигналов.

Специализированные алгоритмы (например, управление кранами) применяются при комплексной отладке системы.

Имитатор может использоваться на трех уровнях архитектуры контроллерного оборудования:

- уровень системной шины — программный имитатор;
- уровень модулей УСО — программно-аппаратный имитатор;
- уровень входных клеммников шкафа автоматики — программно-аппаратный имитатор.

На уровне 1 в контроллер загружается программа-имитатор объекта. На данном уровне производится проверка базового и прикладного программного обеспечения контроллера.

На уровнях 2, 3 используется внешний имитатор, построенный на базе контроллера IUC9000.

На уровне 2 выходы модулей УСО имитатора соединяются с входами модулей УСО контроллеров VME/IUC специализированными кабелями. На

данном уровне производится проверка базового и прикладного программного обеспечения контроллера вместе с модулями УСО.

На уровне 3 выходы модулей УСО имитатора соединяются с входными клеммниками шкафа автоматики специализированными кабелями при комплексной отладке системы. На данном уровне производится проверка базового и прикладного программного обеспечения контроллера, включая модули УСО и весь аппаратный интерфейс шкафа автоматики.

На Рисунке 3.19 и Рисунке 3.20 представлены схемы подключения имитатора к контроллеру на уровнях 2 и 3,

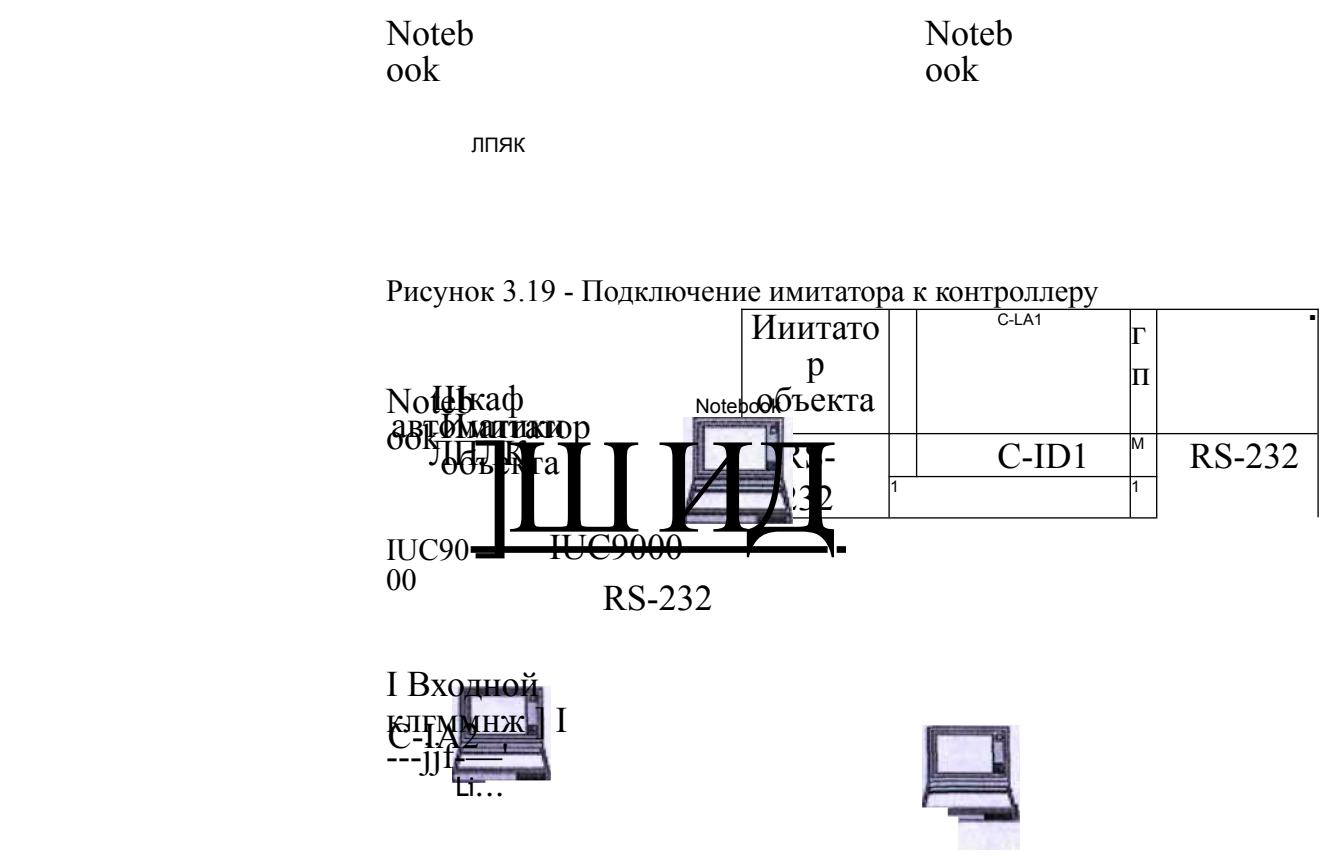
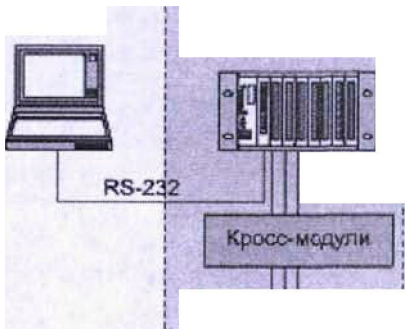


Рисунок 3.19 - Подключение имитатора к контроллеру

Рисунок 3.20 - Подключение имитатора к комплексу

На Рисунке 3.21 дана типовая схема соединений кабелей имитатора объекта для стенда АСУ ТП производства бумвинила «ПХВ-1»



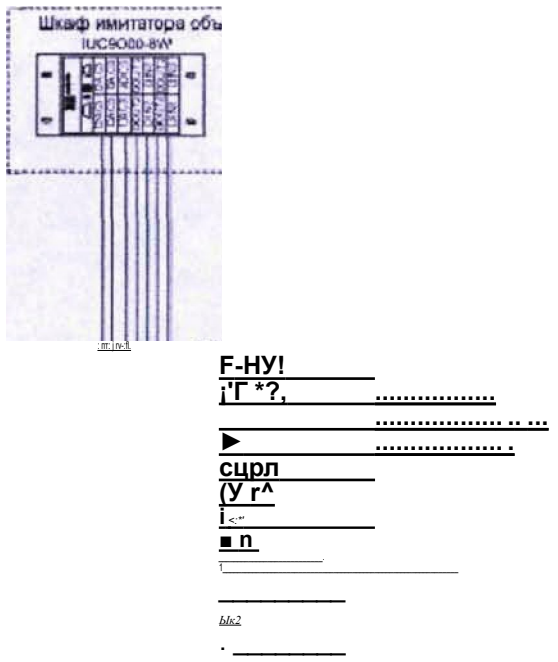


Рисунок 3.21 - Схема соединений кабелей имитатора объекта для стенда АСУТП «ПХВ-1»

Формирование контрольно-измерительных сигналов (КИС) производится с помощью приложения ISaGRAF и других

графических приложений, например, в среде Builder 4.

Формирование контрольно-измерительных сигналов (КИС) производится с помощью приложения ISaGRAF и других графических приложений, например, в среде Builder 4.

Графическое представление программы-имитатора возможно в

графических приложениях с помощью трех типов изображений:

- мнемосхема;
- табличная схема;
- символьная схема.

Пример приложения имитатора в табличной форме представлен на Рисунке 3.22.

L*au >TH 1	LUw THI	Стил ТГИ Т	в*пТ У1	bn.il г» 1 ТС!	KPn Ol
ишлм			В*п ГУ2	И^ЁЯш IC2	КРя ОТА
Lfca uiTM U	ш— тш»		SuiT Yt«	Bww^Viij] 1С«	KPn W

имнгагор пуль- J

| ЦМ>'

Рисунок 3.22 - Приложения имитатора

Базовые графические элементы рисуются, как правило, в любом графическом редакторе и заносятся в поле приложения ISaGRAF. Затем графические элементы привязываются к конкретным дискретным и аналоговым переменным и таким образом становятся

составной частью программы имитатора.

Для отладки системы АСУ ТП необходим комплекс имитаторов.

3.6.3 Комплексная отладка системы

Комплексная отладка системы проводится после её окончательной сборки.

Для организации отладки и проверки собирается

имитатор объекта на базе тех же контроллеров, что используются в основной АСУ ТП. Исполь-зование базовых контроллеров-имитаторов типа IUC9000 (фирма «PEP Modular Computers») чрезвычайно выгодно и удобно как для реализации про-граммного обеспечения задач-имитаторов

объектов, так и для технологической стыковки интерфейсов контрольно-измерительных каналов (КИК). Для данных контроллеров разработано программное обеспечение, эмулирующее работу объекта.

Автор предлагает использовать подобную систему отладки АСУ ТП для моделирования угроз безопасности

, вмешательства в каналы связи, а также защитные мероприятия. Такая система отладки необходима для проведения многочисленных экспериментов и накопления статистики, что иногда невозможно реализовать в реальных условиях в разумные сроки.

В процессе

комплексной отладки имитируются:

- отказы по напряжениям питания;
- изменение питающего напряжения до предельно допустимых значений;
- отказы основных контроллеров (проверка работоспособности резервной аппаратуры);
- поведение объекта путём подачи на модули аналогового и дискретного ввода

сигналов от имитатора;

- имитация отказа (повреждения) основного канала связи;
- имитация НСД в сеть.

3.7 Сравнение результатов отладки (моделирования) до и после введения мер защиты информации в АСУ ТП «ПХВ-1»

Таблица 3.7 содержит результаты экспериментальной отладки АСУ ТП «ПХВ-1» с помощью

контроллеров-имитаторов и задач-имитаторов до и после рекомендованных автором мер защиты. Количество проведенных экспериментов - 100 для каждого параметра.

Таблица 3.7 - Результаты экспериментальной отладки АСУ ТП «ПХВ-1»	До внедрения рекомендованных мер защиты	После внедрения рекомендованных мер защиты
Количество отключений напряжения питания / Количество переключений на резервный источник	100/95	100/ 100
Количество выходов питающего напряжения за предельно допустимые значения / Количество переключений на резервный источник	100/100	100/ 100

Отказы основных контроллеров/ Переключения на резервные	100/94	100/100
Количество превышений технологических уставок / Количество обнаружений превышения	100/92	100/99
Количество превышений аварийных уставок / Количество обнаружений аварий	100/92	100/99
Количество отказов канала связи тОБШив / Количество переключений на резервный канал	100/98	- / (резервный канал исключен)
Количество ошибок в канале связи МОБВШ / Количество потерянных измерений	100/100	100/58 (восстановлены с помощью косвенных измерений)
Количество попыток НСД в канал РЯОРШиЭ / Количество обнаружений НСД	100/74	- / - (НСД в оптоволоконный канал практически не возможен)
Количество попыток НСД в канал МСЮВШ / Количество обнаружений НСД	100/0	100/83

1. Для обеспечения помехозащищенности, достоверности передачи, увеличения пропускной способности канала и защиты от НСД путем физического

подключения **рекомендовано** применение оптической линии связи с кабелем, имеющим соответствующие технические характеристики оптических преобразователей. Это позволит обойтись без резервирования проводного канала связи РЫОРГОиЗ и не увеличит затраты.

Применение оптического РЛОРШиЭ,

при дополнительных затратах на оптическое оборудовании, значительно увеличивает надежность магистрали за счет развязки потенциалов удаленных узлов, защиты от вторичного проявления грозовых токов и обеспечивает высокий уровень защиты от несанк-ционированного доступа (НСД).

Модул
и оптических
преобразоват
елей имеют
встроенную
диагностику
оптического
канала,
индикацию
питания
модуля и
оптического
канала.

2. Пре
образователи
БС/ОС типа
«ИРБИС»,
мощностью
25 Вт, **реко-
мендовано**
заменить на
аналогичные
преобразоват
ели фирмы
«ТЯАСО»,
имеющие
более
высокую
надежность.

3. Для повышения достоверности измерений **рекомендовано** ввести дублирующие вычисления параметров по косвенным характеристикам (например, при измерении расхода жидкостей, газов применяется метод измерения абсолютного давления и разности давлений до и после места сужения трубопровод

а; вместо дифференциального датчика давления целесообразно применить два датчика абсолютного давления и вычислять разность давлений).

ЭСАБА-система МоисЬ, применяемая на предприятии, имеет развитые математические каналы, которые позволяют вести дублирующие вычисления параметров,

но данное преимущество в АСУ ТП не было реализовано разработчиком.

4. Для повышения достоверности измерений (и реализации пункта 3) **рекомендовано** применять интеллектуальные датчики (давления, температуры, уровня, расхода).

5. Для охраны производственного оборудования, защиты от

НСД, пожарной и прочей безопасности, а также для контроля деятельности персонала **рекомендовано** установить систему видеонаблюдения [73].

Угрозы безопасности АСУ ТП «ПХВ-1» и предложенные меры защиты приведены в главе 4 (Таблица 4.3).

3.8 Выводы

1. Исследовано

влияние программных мер защиты на эффективность использования физической скорости передачи в сетях МоёЬш и РгоШэиэ, при применении их на нижнем уровне АСУ ТП. Для характерных на нижнем уровне АСУ ТП коротких сообщений не рекомендуется использовать программные

методы защиты.

2. Проведена экспериментальная проверка защищенности телекоммуникаций нижнего уровня АСУ ТП от НСД с помощью разработанной автором программы.

3. Проведён анализ множества алгоритмов доступа к интеллектуальным сетевым устройствам нижнего

уровня АСУ ТП.

4. Разработаны алгоритмы доступа к узлам сети со стороны пульта и со стороны сети, отличающиеся оптимальным сочетанием методов защиты от НСД и обеспечивающие быстрое обнаружение вторжения. Разработанные алгоритмы реализованы в интеллектуал

ьных датчиках ПД-1ЦМ, ИТ-1ЦМ и приборах ПКЦ-1111, ПКД-1115 (ЗАО «НПП «Автоматика», г. Владимир), применённых в АСУ ТП «ПХВ-1». Акты внедрения приведены в Приложениях.

5. Предложено для сравнительной оценки защищенности узлов сети от НСД использовать отношение

вероятностей уязвимости (преодоления барьера защиты).

6. Экспериментально доказана эффективность разработанных алгоритмов для повышения защищённости узлов сети. Сравнительное экспериментальное исследование нескольких устройств показало многократное (минимум в

5 раз) превосходство по защищённости узлов, в которых реализован разработанный автором алгоритм доступа.

7. Проведено экспериментальное исследование СЗИ АСУ ТП «ПХВ-1».

8. Рекомендовано применение программно-аппаратурных имитаторов на базе контроллеров ПТК для имитации нештатных

ситуаций (сбоев, отказов, НСД), а также защитных мероприятий.

9. Выработаны рекомендации по модернизации системы защиты информации АСУ ТП «ПХВ-1».

4 ОЦЕНКА ЗАЩИЩЕННОСТИ ТЕЛЕКОММУНИКАЦИЙ АСУ ТП

4.1 Методология оценки безопасности информационных технологий по общим (открытым) критериям

На государственном уровне сформулированы критерии, которые позволяют компаниям и госорганам оценивать результаты своей деятельности по защите информации.

С 1999 года во всем мире применяется международный стандарт в области оценки безопасности информационных технологий (ИТ) КОЛЕС 15408 [74-76]. Российский аналог, разработанный в 2002 году - ГОСТР ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности

. Критерии оценки безопасности информационных технологий» [77-79].

Данный стандарт преследует следующие цели:

- Унификация национальных стандартов оценки безопасности ИТ;
- Повышение уровня доверия к оценке безопасности ИТ;
- Сокращение затрат на оценку безопасности ИТ на основе взаимного признания

сертификатов
.
На
основе
данных
стандартов
создаются
профили
защиты,
которые опи-
сывают
требования к
межсетевым
экранам,
АСУ, АСУ
ТП, сайтам и
т.п.
В
поддержку
стандарта
существует
целый ряд
документов.
Среди них:

- Руково
дство по
разработке
защиты и
заданий по
безопасности
[80];

- Процедуры регистрации профилей защиты [81];
- Общая методология оценки безопасности (ОМО) ИТ [82].

В ОМО описываются основные действия, которые необходимо выполнить оценщику при проведении оценки безопасности с использованием критериев и свидетельств оценки.

Данную систему оценок поддерживают многие страны мира, такие как США, Канада, Великобритания, Япония, Россия и другие.

Особенности выполнения количественных оценок. В настоящее время основным подходом к построению критериев оценки безопасности ИТ является использовани

е совокупности определенным образом упорядоченных качественных требований к функциональным механизмам обеспечения безопасности, их эффективности и доверия к реализации.

Качественные критерии применимы для оценки большей части механизмов обеспечения

безопасности ИТ, а также оценки выполнения требований доверия к безопасности изделий ИТ. Несмотря на это, ОМО предусматривает возможность проведения, там где это применимо, количественных оценок с использованием соответствующих качественных показателей.

Чтобы корректно использовать

количественный показатель, он должен иметь объективную интерпретацию, однозначную зависимость от отдельных аспектов безопасности. Поэтому количественные критерии целесообразно использовать для оценки таких механизмов безопасности, как парольная защита, контрольное

суммировани
е и т.п.

Для
оценки
информацио
нной
безопасности
АСУ ТП
автором
разработана
методика
оценки
качества
СЗИ, которая
учитывает
мировые
стандарты
оценки, в том
числе и
ОМО. В
своей оценке
автор
руководстве
тся в том
числе и мето-
дами,
приведенным
и в

документе «Общая методология оценки безопасности информационных технологий».

Нужно отметить, что в ОМО рассмотрены не все вопросы, связанные с оценкой безопасности ИТ, и это обуславливает необходимость дальнейшей разработки дополнительных руководств для всех

участников оценки.

Нормативная база [83-87] в области оценки безопасности ИТ постоянно совершенствуется. В России, то в настоящее время подготовлен проект РД Гос-техкомиссии России «Общая методология оценки безопасности информационных технологий» [88] и проект

«Типовой методики оценки профилей защиты и заданий по безопасности » [89].

4.2 Оценка качества защищённости телекоммуникаций АСУ ТП

Рассмотрим методы оценки качества и выбора рационального варианта СЗИ для телекоммуникаций в АСУ ТП.

4.2.1 Обоснование показателя качества СЗИ.

В общем виде модель процесса защиты информации в АСУ ТП может быть представлена так, как это показано на Рисунке 4.1.

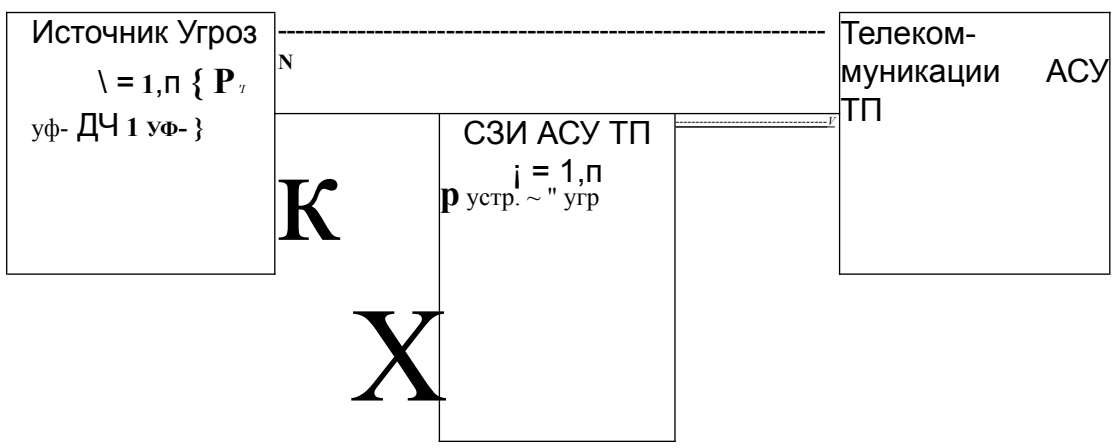


Рисунок 4.1 - Общая модель процесса защиты информации в АСУ ТП

Злоумышленник с помощью некоторого источника угроз (ИУ) генерирует совокупность угроз телекоммуникациям АСУ ТП (путь она будет конечной и счетной 1=1 ..п). Каждая 1-я угроза характеризуе

тся вероятность ю появления $P\{_{угр}$ и ущербом $Дqi^{угр}$■, наносимым системе.

СЗИ выполняет функцию полной или частичной компенсации угроз для телекоммуникаций АСУ ТП.

Основной характеристикой средств защиты являются вероятности устранения каждой ьй угрозы $P_{;\ угр}$ $_{устр}$'.

За счет функционирования СЗИ-обеспечивается уменьшение ущерба XV, наносимого телекоммуникациям АСУ ТП воздействием угроз.

Обозначим общий предотвращенный ущерб через ¡г-, а предотвращенный ущерб за счет ликвидации воздействия ¿-и угрозы через ш/.

После введенных обозначений

сформулируем в общем виде задачу синтеза средств защиты информации в телекоммуникациях АСУ ТП (как это предложено в [31, 32]): Необходимо выбрать вариант реализации СЗИ, обеспечи-вающий максимум предотвращенного ущерба от воздействия угроз при допустимых

затратах на СЗИ.

Формальная постановка задачи имеет вид:

Найти:

$T° = \arg \max F(T), T° \in T^{+}$ (4.2.1)

при ограничении:

$C(T°) < C_{доп}$ (4.2.2)

Здесь T - некоторый вектор, характеризующий вариант технической реализации СЗИ; T^{+},T° - допустимое и оптимальное значение

вектора Т;

Сдоп — допустимые затраты на СЗИ.

Для решения задачи необходимо, прежде всего, сформировать показатель качества функционирования СЗИ *w*(Т).

Предотвращенный ущерб в общем виде выражается соотно

шение

м: $W = F(P_i \cdot$

$Да_i^{ущ} \cdot ?_i^{вер} \cdot i = 1 n)$

$$'^1 iy_{sp} \quad '' ^1 y_{гр}\text{-}^{41} \quad) \qquad (4\ 2\ 3)$$

Предот

вращен

ный

ущерб

за счет

ликвид

ации

воздей

ствия i-

й

угрозы

: $Щ = R_i \cdot A_i^{ущ}$

$P_i^{вер} \cdot i - 1.F$

$$' \ ' у г р \ ' 1 \qquad I_{угр} \qquad (4.2.4)$$

При независимости угроз и аддитивности их последствий получаем:

$$\overline{W} - V P$$

$$-A\ a^{y'гр} \blacksquare P^{усмр}$$

$$i=1$$

(4.2.5)

Останов
вимся
подробно на
сомножителя
х, входящих
в формулу
(4.2.5).
Вероятность
появления і-й
угрозы $P_{j\ угр}$.
определяется
статистическ
и и со-
ответствует
относительн
ой частоте ее
появления:

/
-
1
(
4
.
2
.

6

)

где Л - частота появления i-й угрозы

Ущерб, наносимый i-й угрозой $Aq_{i;}$ может определяться в абсолютных единицах: экономических потерях, временных затратах, объеме уничтоженной или «испорченной» информации и т.д.

Однако, практически

сделать это весьма затруднительно, особенно на ранних этапах проектирования СЗИ [90]. Поэтому целесообразно вместо абсолютного ущерба использовать относительный ущерб, который представляет собой, степень опасности i-й угрозы для телекоммуникаций АСУ ТП. Степень опасности может быть

определена экспертным путем в предположении, что все угрозы составляют полную группу событий [98], т.е.

$$0<A?_{\text{¿}}<1;2>,- =1$$

Сложным вопросом является определение вероятности устранения i-й угрозы $Р_{¡}$ $_{уГ}р^{устр'}$ при проектировании СЗИ. Сделаем допущение, что эта вероятность определяется

тем, насколько полно учтены качественные и количествен-

ные требования к СЗИ при проектирова нии, т.е.

$$P_{угр.} = \blacksquare \blacksquare \bullet , x_{j1},\ldots, x_{jm}) \quad (4.2.7)$$

Где x_{jj} — степень выполнения j-го требования к СЗИ для устранения i-й угрозы, i=l..n; j=l..m.

Пусть первые «Ь>

требований будут количественными (j=l..k), остальные «ш - к» - качественными (pk+1 ..т).

Степень выполнения j-го количественного требования определяется его близостью к требуемому (оптимальному) значению. Для оценки степени выполнения j-го количественного требования к

СЗИ удобнее всего использовать

$$x_{ij} = \frac{x_{ij} - x_{i\min}}{x_{i\max} - x_{i\min}}$$

Как следует из [100], для нормирования можно использовать функцию:

$$x_{ij} = \frac{x_{ij} - x_{i\min}}{x_{i\max} - x_{i\min}} * ,$$

(4

.2

.8

)

где Ху

— текущее

значение]-го

требования;

нл нх

Ху > Ху

- наилучшее

и наихудшее

значения.

С

учетом

формул

ы

(4.2.8)

получа

ем

следую

щие

расчетн

ые

соотно

шения:

при

при

< x <

(4.2.9)

ял _ их

при " *

=----------

(4.2.10)

при X^ >

X^ ; < ^

$$X_a = <$$

$$0?г - {}^{л}у - \qquad (4.2.11)$$

Степень выполнения ^го качественного требования определяется *при* функцией принадлежности к наилучшему значению ц (ху).

Разложив функцию (4.2.7) в ряд Маклорена и ограничившись лишь первыми членами ряда, получим вероятность устранения 1-й угрозы:

т ЗР У"пр

Р $У^{ст}Р$

_ р

$У"»Р$ **/**

П, , V

$^{1}\underline{У^{2}Р}$ **• г**

Пугр -

$Ч_{угр}$ Эх**„**

^{х}И

(4.2.12)

где Р

^{устр}^ угр.(О) =

0 — вероятность устранения ьй угрозы при невыполне-нии требований к СЗИ;

гк " —

величина, характеризующая степень влияния]-го требования на вероятность устранения

1-й угрозы (важность выполнения]-го Требова-ли ния для устранения *i*-*й* угрозы). Очевидно, что *M* для 1=1..п.

После подстановки в (4.2.12) соответствующих значений получаем:

к
т

■/-*+!

(4.2.13)

Окончательно формула (4.2.5) для оценки величины предотвращенного ущерба принимает вид

:

$$\frac{\text{и к}}{\text{п т}}$$

$$= \quad \text{¥}$$

$$x_0 \quad \text{/ч°} \quad \text{'A(]1'}$$

$$+ \quad X$$

$$\text{ХЛ}' \text{ "}$$

° Ч / • }

/

=и=

1

/=1

у=А

+1

(4.

2.1

4)

Таким образом, задача создания СЗИ АСУ ТП в виде (4.2.1),

(4.2.2) сводится к оптимальному обоснованию количественных и качественных требований к СЗИ, при допустимых затратах, и принимает вид:

Найти: шах ил (х^; 1=1..п;]=1..т) (4.2.15)

при ограничении: С(х^) < $С_{Д0П}$\ ¡=1 ..п;]=1 ..т .

В соответствии с формулировкой задачи

(4.2.15)

основными этапами ее решения являются:

- сбор и обработка экспертной информации о характеристиках угроз: частоте появления 1-й угрозы и ущербе Дqj (¡=1 ..п);
- сбор и обработка экспертной информац

ии для определения важности выполнения]-го требования для устранения ьй угрозы ау и функции принадлежности р.(ху), (1=1..п;]=1..т);

- оценка стоимости СЗИ для конкретного варианта ее реализаци

и,
зависящая
от
степени
выполнен
ия
требовани
й C (x^;
1=1..n;]=
1..т);

- выбор
рациональ
ного
варианта
СЗИ АСУ
ТП
(рациональ
ного
задания
тре-
бований)
в
соответст
вии с
постановк
ой (4.2.15)
как задачи
нечеткого

мате-
матическо
го
программ
ирования.

Отмети
м, что при
отсутствии
информации
об угрозах
для решения
задачи
(4.2.15)
может быть
использован
показатель
вида:

$$\frac{\text{"к\_»}\ \text{"I}}{\text{'•=и}}$$

$$\text{=1}$$

$$\text{¡=и=к+}$$

$$\text{\}$$

(4.
2.
16
)

В результате проведенного экспертного опроса были получены следующие показатели, характеризующие степени опасности угроз АСУ ТП «ПХВ-1», относительную частоту их появления, вероятности устранения угроз до и после применения рекомендаций, предложенн

ых автором для защиты. Рассчитан показатель величины относительн ого предотвраще нного ущерба. Данные сведены в Таблице 4.1 и в Таблице 4.2.

Таблица 4.1 - Угрозы безопасности информационной системе и их относительный ущерб от реализации

Угрозы безопасности	Относительный ущерб от ьй угрозы (Степень опасности угрозы) $Д_{чь} 0<Д_{ч},<1$, $1Л_{д},=1$	Вероятность появления ьй угрозы (Отн.частота появл. угрозы) **X*** (»1	Вероятность устранения ьй угрозы $0<Р^{\wedge}_{ф}{}^{устр}<1$	Предотвращенный ущерб от ¡-й угрозы $I\ I_{угр}\ I\ \backslash_{-ср}$
	Экспертная оценка	**Экспертная оценка на основе статистических данных**	**Экспертная оценка на основе статистических данных**	**Расчетные данные**
ический канал связи	0,15	0,08	0,40	0,00048
ие (перебой) питания	0,15	0,23	0,50	0,01725
ой) контроллера	0,10	0,08	0	0
ьная передача данных от некорректная работа	0,20	0,28	0	0
ьство в датчики и ИМ, онированная перенастройка,	0,20	0,15	0,10	0,00300
оте датчиков и ИМ, нарушения цикличности	0,10	0,09	0	0

ограмме (БСАБА)	0,10	0,09	0,1	0,00090
	1-1	1=1		1=0,02163

Таблица 4.2 - Угрозы безопасности

	Относительный ущерб от ¡-й угрозы (Степень опасности угрозы) Дф,0<Дф<1,	Вероятность появления 1-й угрозы (Отн.частота появл. угрозы) **X***	Вероятность устранения 1-й угрозы $0 < P_{;угр}^{устр} < 1$	Предотвращенный ущерб от 1-й угрозы // г.-/;$_{и\,Iугр}$ '
	Экспертная оценка	**Экспертная оценка на основе статистических данных**	**Экспертная оценка на основе статистических данных**	**Расчетные данные**
ический канал связи	0,15	0,08	0,97	0,01164
ие (перебой) питания	0,15	0,23	0,90	0,03105
й)контроллера	0,10	0,08	0,99	0,02277
ная передача данных от накорректная работа	0,20	0,28	0,96	0,05376
ство в датчики и ИМ, нированная перенастройка,	0,20	0,15	0,99	0,02970
боте датчиков и ИМ, е нарушения цикличности	0,10	0,09	0,99	0,00891
ограмме (ЗСАОА)	0,10	0,09	0,99	0,00891
	1=1	1=1		1= 0,16674

Таблица 4.3 - Угрозы безопасности и меры защиты по защите

Угроза безопасности	Мера защиты от данной угрозы	Реализация мер защиты	Внутренние или внешние средства ща- шиты
ический канал связи	Применение оптоволоконной линии связи	Аппаратурная	Внутренняя
ие (перебой) питания	Резервирование питания, применение более надежных источников бесперебойного питания	Аппаратурная	Внешняя
й)контроллера	Применение резервных контроллеров	Аппаратурная	Внешняя
ная передача данных от датчиков ная работа датчиков)	Применение дублирующих вычислений параметров ко косвенным характеристикам	Программная	Внутренняя

льство в датчики и ИМ, онированная перенастройка, сбой в	Применение интеллектуальных датчиков и приборов: - применение процедурного и числового паролей для доступа к настройкам датчиков и ИМ с пульта - открытие сетевого доступа к настройкам только с пульта - автоматическое закрытие доступа (по истечении определенного времени) - закрытие доступа к настройкам командой по сети - передача байта статуса в каждом ответе (отображает факт перенастройки прибора)	Аппаратурная	Внутренняя
боте датчиков и ИМ, вследствие я цикличности работы	Отслеживание цикличности работы интеллектуальных узлов, применение локальных сторожевых таймеров	Аппаратурная	Внутренняя
ограмме (БСАОА)	Отслеживание цикличности работы программ и обмена по сетям, применение системных сторожевых таймеров	Программная	Внутренняя

Предотвращенный ущерб от 1-й угрозы до и после применения рекомендаций по защите показан на Рисунке 4.2.

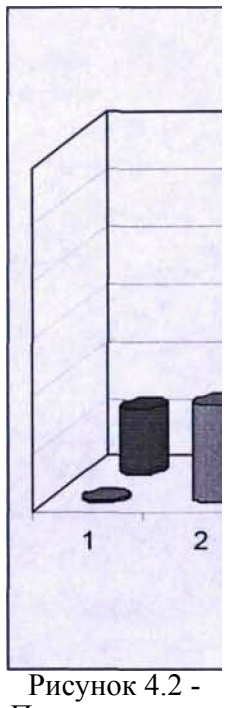
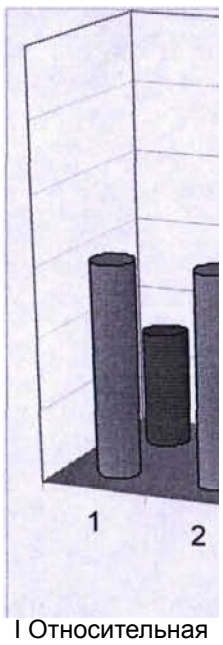


Рисунок 4.2 - Предотвращенный ущерб от 1-й угрозы

Относительная опасность (относительный ущерб) и относительная частота появления (вероятность появления) ¡-й угрозы представлены на Рисунке 4.3.



I Относительная опасность угрозы
■ Относительная частота появления

Рисунок 4.3 - Относительная опасность и относительная частота появления ¡-й угрозы

4.3 Определение важности требований, предъявляемых к СЗИ

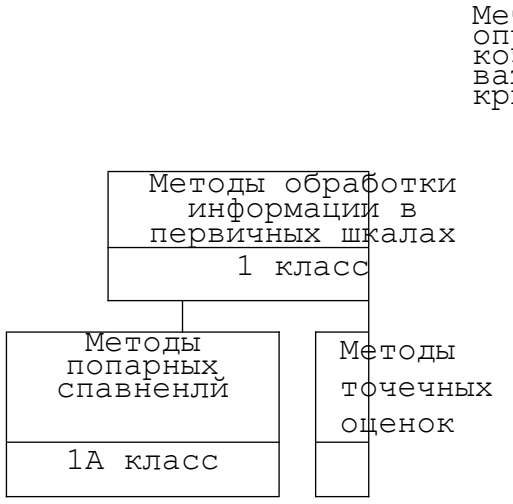
При выборе наилучшего варианта системы защиты информации в соот-ветствии с полученым

нами критерием, возникает задача определения важности (веса) требований, предъявляемых к параметрам СЗИ.

Наиболее полный обзор методов определения коэффициентов важности приведен в литературе [98].

Иерархическая классификация методов определения коэффициент

ов важности требований приведена на Рисунке 4.4.



Методы обработки информации в проичводньгх шкалах
2 класс

Методы аппроксимации функции полезности	Методы трансформации частот
2А класс	2Б класс

*атраины	Ри рожие иетэги
1А.1	
1Б.1	1Б.2

М» гиды	Мґоли $утаф1*	'УЪ>ШМ1С1Й*	Методы травеформвиси топш>г**вм	М-тш тр«нс (юрмасни ътсеу'ея	Методы аагторо* ССшномиампА
2А. 1	2А. 2	2А. 3	2Б. 1	2Б. 2	2Б.З

1А. 2.	
СО&ТМИШ	
1АЛ .	

1АЛ
.

1Б. 2Л	

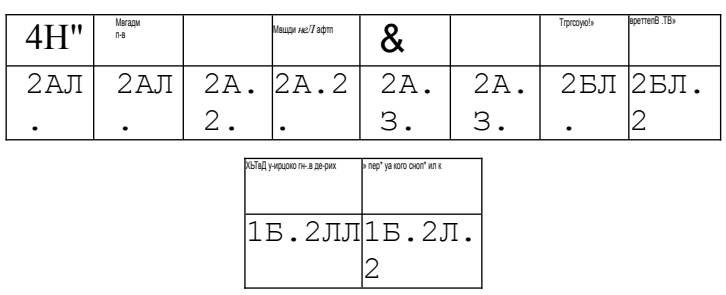


Рисунок 4.4 - Иерархическая классификация методов определения коэффициентов важности критериев

При решении практических задач обоснования требований и оценки сис-тем защиты информации возникает вопрос рациональног о выбора метода оп-ределения весовых коэффициент ов из числа 19 групп изложенных в [98-102] методов. Неправильны й выбор метода приводит к недостаточно й обоснованно-

сти
производимы
х операций
над
малодостовер
ными
исходными
экспертными
данными

.

Автором решается задача выработки рекомендаций для проектировщиков АСУ ТП малой и средней сложности. Проектировщики таких АСУ ТП как правило представляют из себя малые предприятия, с числом сотрудников от 5 до 10. Решения принимает директор предприятия, реже — ведущий специалист. Поэтому главным критерием выбора метода оценки следует принимать простоту получения экспертных данных при высокой степени согласованности мнений экспертов и при минимальном количестве экспертов.

Поэтому автором проведен анализ методов определения весовых коэффициентов с целью выбора наиболее подходящих для решения задачи определения важности требований, предъявляемых к СЗИ АСУ ТП.

Анализ литературы [98, 106 и др.] позволяет определить основные факторы, влияющие на выбор метода оценки весовых коэффициентов. Рассмотрим эти факторы.

1. Физическая сущность параметров и отношение между ними.

Параметры (в нашем случае требования к СЗИ) определяются исходя из

смысла провозглашенной цели. Далее необходимо определить степень взаимосвязей между ними, т.е. зависимости или независимости. Характер зависимости или независимости (независимость по полезности, по предпочтению, по безразличию и т.д.) влияет на выбор метода оценки.

2. Сложность проведения экспертизы и трудоемкость получения экспертной информации.

Сложность и трудоемкость экспертизы определяется реальными условиями и возможностями ее проведения.

Как показано в [98], наименьшего времени общения с экспертами требует ранжирование и метод Терстоуна; метод линейной свертки требует

наибольшего времени общения с экспертами (в 12 раз больше, чем ранжирование; в 2 раза больше, чем метод Черчмена-Акофа) и т.д.

3. Степень согласованности мнений экспертов.

Степень согласованности в зависит от количества привлекаемых экспертов и уровня их квалификации. В то же время на нее влияет выбранный метод оценки весов. Так, наибольшую согласованность экспертов обеспечивает линейная свертка, наименьшую - непосредственная численная оценка весов, при этом ранжирование при его простоте позволяет получить весовые коэффициенты достаточно точные и близкие к их значению, полученному методом линейной свертки.

4. Трудоемкость обработки экспертных данных.

Этот фактор не является главным при современном уровне развития вычислительной техники. Однако, применение сложных методов обработки экспертной информации может потребовать разработки специальной программы обработки, что повлияет на сроки проведения экспертизы. Очевидно, что наиболее простыми методами с этой точки зрения являются ранговые методы и балльные методы.

Учет приведенных факторов позволяет на практике выбрать рациональный вариант оценки весовых коэффициентов применительно к СЗИ АСУ ТП. Метод Саати, по мнению автора, является оптимальным по совокупности факторов для поставленной задачи.

4.3.1 Определение важности требований, предъявляемых к СЗИ, методом Саати

Суть метода: Результаты попарного сравнения параметров описываются отношениями их весов, т.е. представимы в виде матрицы А (матрицы Саати).

А = || / Ау ||; уе1..п.

$$A = \text{Я}_2 / \text{Я}, \ 1 \ldots \text{ЫК} \qquad (43Л)$$

4,/я, к'к - 1

Справедливо следующее равенство [101],

$$(A - \pi E)'A = 0 \qquad (4.3.2)$$

где Е - единичная матрица; А - вектор весов.

Для нахождения вектора весов Л необходимо решить уравнение (4.3.2). Поскольку ранг матрицы равен 1, то п — единственное собственное число этой матрицы и, следовательно, уравнение (4.3.2) имеет ненулевое решение. Более того, это единственное решение, обладающее свойством: ⁼ 1-

Это решение и есть искомый вектор относительных весов параметров — вектор Саати.

Определим коэффициенты важности требований, предъявляемых к СЗИ АСУ ТП «ПХВ-1», на основе метода парных сравнений (метода Саати). Шкала для оценки относительной важности требований приведена в Таблице 4.4.

Таблица 4.4 - Шкала относительной важности требований **Интенсивность относительной важности**	**Определение**
1	Равная важность сравниваемых требований
3	Умеренное (слабое) превосходство одного над другим
5	Сильное (существенное) превосходство
7	Очевидное превосходство
9	Абсолютное (подавляющее) превосходство
2,4, 6,8	Промежуточные решения между двумя соседними оценками

Основными при выборе СЗИ «ПХВ-1» являются следующие требования:

- к аппаратным средствам защиты информации;
- к программным средствам защиты информации;
- к структуре АСУ ТП;
- к нормативной базе, документации на АСУ ТП.

$$A = \begin{matrix} 1 & 5 & \mathbf{6} \\ 1/5 & 1 & \\ 1/6 & & 4 \\ 1/7 & 1/6 & 1/4 \quad 1 \end{matrix}$$

Как следует из соотношения (4.3.2), необходимо решить задачу нахождения собственных значений (А - Х Е) • \У = 0, где \У - собственный вектор, а А, —

Определим относительную важность 4 требований к СЗИ «ПХВ-1». В результате экспертного опроса получена следующая матрица парных сравнений:

собственное значение матрицы. Эта неоднородная система имеет нетривиальное решение тогда и только тогда, когда определитель матрицы (А - X Е) равен нулю. Найдем его:

1 -Л 5 6 7
1/5 1 -Л 4 6
1/6 1/4 1-Я 4
1/7 1/6 1/4 1 - Я

Уравнение имеет решение:

А, 1 = — 0,362; X_2 = -0,140+ 1,3051; X_3 =-0,140 - 1,3051; A_4 = 4,390. Следовательно, X_{max} = 4,390. Найдем соответствующий вектор:

= 0

- 4,390	5	6	7	¿У, со$_2$ б»$_4$
1/5	1 - 4,390	4	6	
1/6	1/4	1-4,390	4	
1/7	1/6	1/4	1- 4,390	

Введем условие нормировки (л)$_1$+ш$_2$+Шз+1л)4=1. Рассмотрим систему:

- 3,390«, + 5а>$_2$ + 6щ + 7бУ$_4$ = 0 0,2бУ, - 3,390й>$_2$ + 4й), + 6гу$_4$ = 0
0,166«, + 0,25«$_2$ - 3,390гУ$_3$ + 4а)$_4$ = 0 0,142«, + 0,166й>$_2$ + 0,25й>$_3$ - 3,390й>$_4$ =0

Система (*) имеет только нулевое решение. Для нахождения собственного вектора АЛ^ используется замена одного из уравнений (*) условием нормировки. В результате решения системы получаем собственный вектор весов: = (СО,, С0$_2$, ш$_3$, СО4), СО] = 0,619, ш$_2$= 0,235, 0)$_3$= 0,101, (А)$_4$ = 0,045.

Отметим, что матрица парных сравнений отражает согласованные суждения тогда и только тогда, когда X $_{max}$ = п. Кроме того, всегда X $_{max}$ > п, поэтому max - п) дает меру несогласованности и указывает, когда суждение экспертов следует проверить. При п=4, X_{max} - 4,390, мера несогласованности = Л⁴ -4Я³ -6,914^-2,715 = О равна 0,390.

Индекс согласованности (ИС), который отражает качество экспертных оценок, рассчитываем по формуле: X-п

ИС =

ИС = (4,39 — 4) / (4 — 1) = 0,13.

Средние согласованности (СС) для матриц случайного порядка приведены в Таблице 4.5.

Таблица 4.5 – Средние согласованности для матриц случайного порядка *n*	1	2	**o** o	4	5	6	7	8	9	10
CC	0	0	0,58	0,90	1,12	1.24	1,32	1,41	1,45	1,49

Общая рассогласованность (ОС) рассчитывается следующим образом:

$$OC = \frac{ИС}{CC} 100\%$$

ОС = (0,13 / 0,9) • 100% = 14,4%.

Согласно методу Саати величина ОС должна быть не более 20%, в противном случае, такие суждения экспертов следует перепроверить.

В нашем случае мера несогласованности равна 0,39 что является допустимым при принятой шкале (Таблица 4.4), показатель ОС равен 14,4%, что не превышает допустимого порога рассогласованности.

Определение весовых коэффициентов с помощью нахождения вектора XV матрицы парных сравнений является довольно трудоемкой задачей. Для решения практических задач можно [94, 97] определять весовые

коэффициенты путем расчета среднего геометрического из соотношения:

$$Щ = н||\sim 2оу\ ;/ = 1.и, \qquad (4.3.3)$$

где а^ - коэффициенты матрицы парных сравнений.

Рассчитаем весовые коэффициенты методом среднего геометрического:

	X,	x_2	X_3	X4	П*и		^{4}л/Пху/£
X,	1	5	6	7	210	3,80	0,614
x_2	0,200	1	4	6	4,8	1,48	0,239
X_3	0,166	0,250	1	4	0,166	0,64	0,103
X,	0,142	0,166	0,250	1	0,00589	0,27	0,044
					1=	6,19	1,000

В нашем случае получаем: 0)1 = 0,614, $C0_2$ = 0,23 9, co_3= 0,103, co_4= 0,044.

Ошибки определения весовых коэффициентов не превышают 5%, что говорит о возможности применения данного метода.

В соответствии с Таблицей 4.4 мы получили сильное превосходство одного требования над другим. Это говорит о том, что есть более важные требования и мене важные. Есть явно выраженное главное требование - к аппаратным СЗИ, а также незначительное требование - к нормативной базе АСУ ТП.

Рассчитанная относительная важность требований к СЗИ АСУ ТП «ПХВ- 1» в процентах приведена в Таблице 4.6.

Таблица 4.6 - Относительная важность требований к СЗИ АСУ ТП «ПХВ-1» **Требования к СЗИ АСУ ТП**	**Относительная важность**
к аппаратным средствам защиты информации	61,4%
к программным средствам защиты информации	23,9%
к структуре АСУ ТП	10,3%
к нормативной базе, документации на АСУ ТП	4,4%

4.4 Построение функции принадлежности

В случае если экспертная оценка имеет качественное выражение, тогда оценки вариантов по критериям и коэффициенты относительной важности задаются функциями принадлежности.

Существует значительное количество методов построения по экспертным оценкам функций принадлежности нечеткого множества ц. ^{л}(х). Выделяют две группы методов: прямые и косвенные методы [94].

Прямые методы характеризуются тем, что эксперт непосредственно задает правила определения значений функции принадлежности ц. ^{л}(х), характеризующей элемент х. Эти значения согласуются с его предпочтениями на множестве элементов X следующим образом:

-для любых $x_ь$ x_2 е X, ц. ^{л}(X]) < ц. ^{л}(x_2) тогда и только тогда, когда x_2 предпочтительнее $x_ь$ т.е. в большей степени характеризуется свойством А;

- для любых $x_ь$ Хг е X, р. ^{л}(х1) = ц. ^{л}(x_2) тогда и только тогда, когда X] и x_2 безразличны относительно свойства А.

Примерами прямых методов являются непосредственное задание функции принадлежности таблицей, графиком или формулой. Недостатком этой группы методов является большая доля субъективизма.

В косвенных методах значения функции принадлежности выбираются таким образом, чтобы удовлетворить заранее сформулированным условиям. Экспертная информация является только исходной информацией для дальнейшей обработки. Дополнительные условия могут налагаться как на вид получаемой информации, так и на процедуру обработки.

Поэтому автором проанализированы косвенные методы построения функций принадлежности, из которых был отобран метод ранговых оценок. Главным преимуществом данного метода является то, что в отличие от метода парных сравнений, он не требует решения характеристического уравнения, а позволяет вычислять функции принадлежности с использованием ранговых оценок, которые достаточно легко получить при экспертном опросе. Данный метод обладает достаточной точностью вычислений и позволяет легко автоматизировать расчеты.

4.4.1 Построение функции принадлежности на основе ранговых оценок

Данный метод базируется на идее распределения степени принадлежности элементов универсального множества согласно с их рангами.

Будем понимать под рангом элемента x;eX число $r_3(x])$, которое характеризует значимость этого элемента в формировании свойства,

r1
r1

которое описывается нечетким термом 8. Допускаем, что выполняется правило: чем больший ранг элемента, тем больше степень принадлежности.

Введем также обозначения: $r_3(x^ = r;; |a_5(x_!) = ; I = 1 ..n.$

Тогда правило распределения степеней принадлежности можно задать в виде соотношения:

$$^{Г2} \qquad ^{r}» \qquad (4.4.1)$$

к которому добавляется условие нормирования:

$$ц, + ц_2+... + ц_п=1 \qquad (4.4.2)$$

Используя соотношение (4.4.1) легко определить степени принадлежности всех элементов универсального множества через степени принадлежности опорного элемента.

Если опорным элементом является X] е X с принадлежностью ц

ь то: а Л

$$A = — ■ A ; A = — ■■ A A , = — ■ A \qquad (4.4.3)$$

Для опорного элемента x_2 е X с принадлежностью $\backslash x_2$, получаем:

$$A = \sim " A \wedge A = \sim " A \wedge ■ ■ ■ \wedge A = \sim " A \qquad (4.4.4)$$

Го Го Го

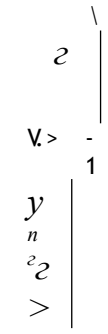
Для опорного элемента $x_{„} e X c$ принадлежностью $ц_п$,

имеем: г, г7 г,

$$M1 = --M»>M2 = --M»>-'>M_п-, = —-A \qquad (4.4.5)$$

r" r» r»

Учитывая условие нормировки (4.4.2) из соотношений (4.4.3) - (4.4.5) находим:



Полученные формулы (4.4.6) дают возможность вычислять степени принадлежности ц $_{8}$(x;) двумя независимыми путями:

- по абсолютным оценкам уровней г;; 1=1 ..п , которые определяются по 9- бальной шкале (1 — наименьший ранг, 9 - наибольший ранг).

по относительным оценкам рангов т\/ х\ = a_{1} ; 1,] = 1..п, которые образуют матрицу

:

-

$$l_1 u$$

$$>2\ Ъ$$

$$Г\ Г\ Г\ n'\ n\ n$$

(4.4.7)

Эта матрица обладает следующими свойствами:

а) она диагональная, т.е. ан=1; ¡=Т..п;

б) элементы, которые симметричны относительно главной диагонали, связаны зависимостью: ау=1 / а^^;

в) она транзитивна, т.е. а^. $a_{кl}$, поскольку

$$П\ ^{г}к\ \_\ Ъ$$

') О

Наличие этих свойств приводит к тому, что при известных элементах одной строки матрицы А легко определить элементы всех других строк. Если известна г-я строка, т.е. элементы а^, к;]=1..п, то произвольный элемент щ находится так:

ªУ> ⁼ / ª1т Ь --П

Поскольку матрица (4.4.7) может быть интерпретирована как матрица парных сравнений рангов, то для экспертных оценок элементов этой матрицы можно использовать 9-бальную шкалу Саати: щ = г; / Эта шкала приведена ранее, в Таблице 4.4.

Таким образом, с помощью полученных формул (4.4.6), экспертные значения о рангах элементов или их парные сравнения преобразуются в функцию принадлежности нечеткого терма [93].

Алгоритм построения функции принадлежности включает в себя следующие операции:

1) Задать лингвистическую переменную;

Определить универсальное множество, на котором задается лингвистическая переменная;

2)

$A =$ 3) Задать совокупность нечетких термов {$8_ь$ 8_2, ... , $8_т$}, которые исп

ользуются для оценки переменной;

4) Для каждого терма 8^]=1..ш сформировать матрицу (4.4.7);

5) Используя формулы (4.4.6) вычислить элементы функций принадлежности для каждого терма.

Нормирование найденных функций осуществляется путем деления на наибольшие степени принадлежности.

Функции принадлежности применяются при выборе рационального варианта СЗИ (п. 4.5.3), а также при определении важности требований к СЗИ в случае, когда экспертные оценки заданы в качественной форме.

4.5 Выбор рационального варианта СЗИ на основе экспертных оценок

4.5.1 Анализ методов выбора рационального варианта СЗИ

Принципиальными особенностями решения задачи выбора рационального варианта СЗИ, определяющими метод ее решения являются [112-114]:

- многокритериальное^ задачи выбора;
- не только количественное, но и качественное (нечеткое) описание показателей качества СЗИ, задаваемых в виде требований;
- при нечеткой постановке задачи влияние на выбор метода ее решения экспертной информации, определяющей предпочтение того или иного показателя [91-93].

Рассмотрим указанные особенности решения задачи более подробно. Общая постановка задачи многокритериальной оптимизации [97]: Пусть X — | $x_ь$...,$x_;$,...,$x_п$| - вектор оптимизируемых параметров некоторой системы 8. Некоторое]-е свойство системы 8 характеризуется величиной]-го показателя ^(X);] = 1„т. Тогда система в целом характеризуется вектором показателей О = Задача многокритериальной оптимизации сводится

к тому, чтобы из множества M_5 вариантов системы 8 выбрать такой вариант (систему 8о), который обладает наилучшим значением вектора р. При этом предполагается, что понятие «наилучший вектор предварительно сформулированно математически, т.е. выбран (обоснован) соответствующий критерий предпочтения (отношение предпочтения).

Анализ литературы [106, 107] показывает, что все многочисленные методы решения многокритериальных задач можно свести к трем группам методов:

- метод главного показателя качества;
- метод результирующего показателя качества (аддитивного, мультипликативного, максиминного);
- лексикографический метод (метод последовательных уступок).

Принципиальной особенностью рассматриваемой задачи выбора рационального варианта СЗИ АСУ ТП является преимущественно качественный характер показателей, трактуемых как требования к СЗИ. В связи с этим рассматриваемые методы многокритериальной оптимизации должны формулироваться в нечеткой постановке.

Как в классической, так и в нечеткой постановке выбор метода решения многокритериальной задачи определяется тем, в каком виде представлена экспертная информация о предпочтении показателей или их важности. Для этого приведем таблицу, которая позволяет обоснованно выбирать метод нечеткой многокритериальной оптимизации в зависимости от экспертной информации о предпочтении показателей (Таблица 4.7).

Таблица 4.7 Выбор метода решения в зависимости от экспертной информации **Экспертная информация о степени предпочтения или важности показателей**	**Метод решения многокритериальной задачи**
отсутствует	максиминный метод
показатели упорядочены по важности	лексикографический метод
определены весовые коэффициенты показателей	аддитивный показатель мультипликативный показатель максиминный показатель

4.5.2 Выбор варианта СЗИ по аддитивному показателю

Поскольку, в нашем случае весовые коэффициенты показателей качества СЗИ определены — используем метод аддитивного показателя для выбора оптимального варианта СЗИ «ПХВ-1».

Метод результирующего показателя качества основан на формировании обобщенного показателя путем интуитивных оценок влияния частных показателей качества ..., на результирующее качество выполнения системой ее функций. Оценки такого влияния даются группой специалистов - экспертов, имеющих опыт разработки подобных систем.

Наибольшее применение среди результирующих показателей качества получили аддитивный, мультипликативный и минимаксный показатели.

Аддитивный показатель качества представляет собой сумму взвешенных нормированных частных показателей и имеет вид:

^{m}

$$\hat{} \ , \qquad (4.5.1)$$

где ^{c*3} — нормированное значение]-го показателя;

С^ - весовой коэффициент]-го показателя, имеющий тем большую величину, чем больше он влияет на качество системы. =1; > 0;] = 1..ш.

Для 5 вариантов СЗИ «ПХВ-1» в результате экспертного опроса получены данные о степени выполнения каждого из 4 показателей качества.

Варианты оцениваются по 4 требованиям (критериям), описанным выше (п. 4.3.1): С1 - требования к аппаратным СЗИ, C_2 — требования к программным СЗИ, Сз - требования к структуре, С4 — требования к нормативной базе. С, = { 0,9/аь 0,9/a_2; 0,8/a_3; 0,6/a_4; 0,7/a_5 } C_2 = { 0,8/аь 0,9/a_2; 0,7/a_3; 0,8/a_4; 0,9/a_5 } C_3 = { 0,5/аь 0,7/a_2; 0,8/a_3; 0,9/a_4; 0,8/a_5 } C_4 = { 0,6/а,; 0,7/a_2; 0,6/a_3; 0,7/a_4; 0,4/a_5 }

Расчет аддитивного показателя качества СЗИ «ПХВ-1» по формуле (4.5.1) приведен в Таблице 4.8.

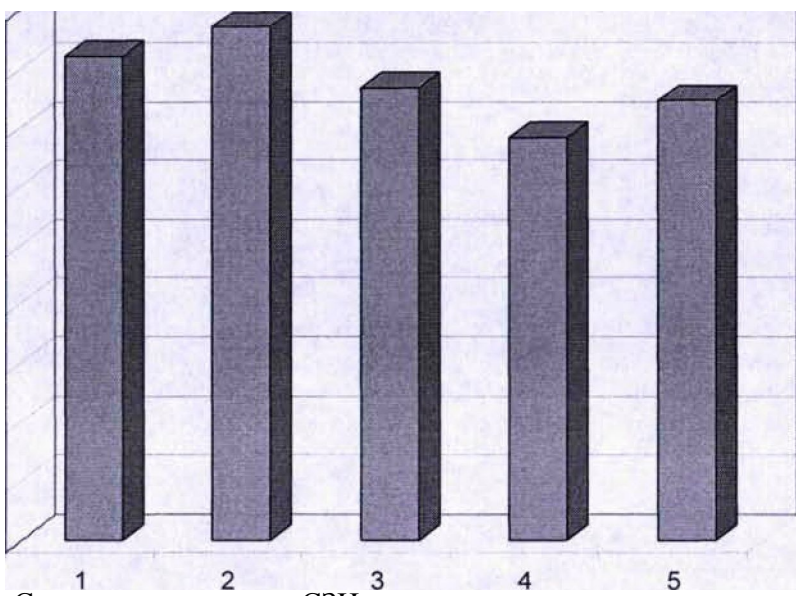
Таблица 4.8 - Расчет аддитивного показателя качества СЗИ «ПХВ-1»	**СЗИ,**	$сзи_2$	**СЗИз**	$сзи_4$	$сзи_5$	**Отн. Вес. показателя качества**
С,	0,9	0,9	0,8	0,6	0,7	0,614
c_2	0,8	0,9	0,7	0.8	0,9	0,239
Сз	0,5	0,7	0,8	0,9	0,8	0,103
c_4	0,6	0,7	0,6	0,7	0,4	0,044
Аддитивный показатель	0,8217	0,8706	0,7673	0,6831	0,7449	

Сравнение вариантов СЗИ по аддитивному показателям» уровня качества представлено на графике (Рисунок 4.5).

0,9

0,5

0,1



0,8 0,7 0.6

0,4 0,3 **0,2**

0

Рисунок 4.5 - Сравнение вариантов СЗИ по аддитивному показателяю уровня качества

Таким образом, наилучшим является второй вариант СЗИ. По графику (Рисунок 4.5) легко определить, насколько тот или иной вариант защиты соответствует обобщенным требованиям.

4.5.3 Выбор варианта СЗИ при задании требований в качественной форме

Если оценки вариантов по критериям и коэффициенты относительной

важности задаются функциями принадлежности соответственно и

$Vw^j)$

Необходимо упорядочить m вариантов СЗИ $a_ь$ a_2, ..., $a_т$, оцениваемых по «п» требованиям (критериям) Сь Сг, ..., $С_п$. Соответствующую оценку обозначим Ry; i=l..m, j=l..n. Относительная важность каждого требования задается коэффициентом Wj , £Wj =1. В этом случае взвешенная оценка i-ro варианта вычисляется по формуле: u

$$/=1 \qquad (4.5.2)$$

Так как в данном случае Ry и Wj являются нечеткими числами, Rj определяется в соответствии с формулой (4.5.2) на основе принципа обобщения. Бинарную операцию * (в данном случае это операция сложения или умножения) можно обобщить на случай нечетких чисел (например, X и Y), задаваемых функциями принадлежности $ц._x(x)$ и ц.у(у) соответственно. Результат обобщенной операции * - нечеткое число Z, определяемое функцией принадлежности:

$$fi_z(z) = \sup \min(//_v(.x),/i_K \qquad (4.5.3)$$

г-**у

После того, как взвешенные оценки R; получены, необходимо сравнить варианты на их основе. Для этого вводится нечеткое множество I, заданное на множестве индексов вариантов {1, 2, ..., ш}. Значение соответствующей функции принадлежности интерпретируется как характеристика степени того, насколько вариант $a\backslash$ является лучшим. Значение ji ¡(1) вычисляется по формуле:

$$¡л_т\{/) = \sup millДд\ (ry) \qquad (4.5.4)$$

>

4.5.4 Выбор варианта СЗИ лексикографическим методом

В случае, если весовые коэффициенты показателей не определены, но упорядочены по важности — возможно использование лексикографического метода выбора [105]. Данный метод, в отличие от метода аддитивного

показателя, позволяет только определить какой из вариантов СЗИ лучше, но не возво- ляет определить на сколько.

Суть метода заключается в выделении сначала множества альтернатив с наилучшей оценкой по наиболее важному показателю. Если такая альтернатива единственная, то она считается наилучшей; если их несколько, то из их подмножества выделяются те, которые имеют лучшую оценку по второму показателю и т.д.

Для расширения множества рассматриваемых альтернатив и улучшения качества решения по совокупности показателей может назначаться уступка, в пределах которой альтернативы считаются эквивалентными.

Применение этого метода при нечетких показателях качества (требованиях) СЗИ сводится к следующим операциям [113].

1) Упорядочить требования к СЗИ по важности:

Ci > C_2 > ... > Cj > ... > C_n; j = l..n.

2) С согласия ЛПР для каждого требования назначается величина допус- тимой уступки ACj; j = l..n. в пределах которой рассматриваемые варианты СЗИ считаются «практически равноценными».

3) Для первого требования C] формируется множество «практически рав- ноценных» вариантов, удовлетворяющих условию - множество щ.

t^{*i}

4) Если тс 1 - множество содержит ровно один вариант, то он и считается наилучшим. Если щ - множество содержит более одной альтернативы, то переходим к рассмотрению всех вариантов множества tïi по требованию C_2.

5) Для второго требования C_2 формируется 7Ь ~ множество вариантов из множества к ь удовлетворяющих условию:

max .Л'с, (а^) - /fc (a_k) < tC-,

Л-

6) Если 712 ~ множество содержит ровно один вариант, то он и считается наилучшим; если более одного - рассматриваем эти варианты по требованию C_3 и т.д.

7) Если все требования последовательно пересмотрены и в результате получаем 7Г — множество % = щ • • ... ■ 7С„ содержащее более одной альтернативы, то возможно применить два подхода:

- уменьшить величину допустимой уступки А Cj, начиная с первого по важности требования и повторить все шаги решения;
- представить ЛПР окончательный выбор лучшего варианта.

Выбираем наиболее подходящий из 5 вариантов СЗИ «ПХВ-1» (aj) лексикографическим методом.

Варианты оцениваются по 4 требованиям (критериям), описанным выше (п. 4.3.1): Ci - требования к аппаратным СЗИ, C_2 - требования к программным СЗИ, C_3 - требования к структуре, C_4 - требования к нормативной базе.

В результате экспертной оценки получены следующие данные, характеризующие степень соответствия СЗИ заданным требованиям:

$C_1 = \{ 0,9/a_1\ 0,9/a_2;\ 0,8/a_3;\ 0,6/a_4;\ 0,7/a_5 \}$

$C_2 = \{ 0,8/a_1;\ 0,9/a_2;\ 0,7/a_3;\ 0,8/a_4;\ 0,9/a_5 \}$

$C_3 = \{ 0,5/a_1\ 0,7/a_2;\ 0,8/a_3;\ 0,9/a_4;\ 0,8/a_5 \}$

$C_4 = \{ 0,6/a_1;\ 0,7/a_2;\ 0,6/a_3;\ 0,7/a_4;\ 0,4/a_5 \}$

1) Требования упорядочены по важности следующим образом:

$C_1 > C_2 > C_3 > C_4$

2) Зададимся величиной допустимой уступки:

A Cj = 0,1 для всех $P_{;\ угр}$.

3) Формируем множество по первому требованию. При максимальном значении Ci = 0,9 и A Ci = 0,1 в это множество входят варианты $Л_1$ = {a_1 a_2, a_3}.

4) Из элементов множества л\ формируем множество %$_2$ по второму требованию. При шах C_2=0,9 **и** А C_2 = 0,1 — множество 7и$_2$ = {а$_ь$ а$_2$}.

5) Из элементов множества *л* = *щ* • *л$_2$* формируем множество *л$_3$* по третьему требованию. При C_3=0,7 и А C_3 = 0,1 - это множество содержит один элемент *л$_3$* — а$_2$.

Таким образом, наилучшим является второй вариант СЗИ.

4.6 Выводы

1. Выработаны рекомендации по оценке СЗИ для проектировщиков АСУ ТП малой и средней сложности на основе методологии оценки безопасности ИТ по общим критериям (ГОСТ Р ИСО/МЭК 15408-2002).

2. Обоснован показатель качества СЗИ АСУ ТП — уменьшение общего ущерба, наносимого воздействием угроз.

3. Разработана методика оценки защищенности АСУ ТП, включающая в себя выбор и обоснование методов определения важности требований, предъявляемых к СЗИ, построения функции принадлежности СЗИ к заданному уровню качества, а также выбора рационального варианта СЗИ из нескольких возможных.

4. Проведена оценка СЗИ АСУ ТП «ПХВ-1» согласно разработанной методике оценки СЗИ, выбран наилучший вариант СЗИ.

ЗАКЛЮЧЕНИЕ

Основные результаты диссертационной работы:

1. Предложен подход к построению СЗИ, при котором внешняя защитная оболочка должна дополняться встроенными механизмами защиты оборудования и телекоммуникаций на всех уровнях АСУ ТП.

2. Разработана методика создания СЗИ, учитывающая использование встроенных механизмов защиты оборудования и телекоммуникаций, следование нормативно-правовой базе в области ИБ, оформление СЗИ, как подсистемы АСУ ТП.

3. Разработаны алгоритмы доступа к узлам сети со стороны пульта и со стороны сети, отличающиеся оптимальным сочетанием методов защиты от НСД и обеспечивающие быстрое обнаружение вторжения. Разработанные алгоритмы реализованы в интеллектуальных датчиках ПД-1ЦМ, ИТ-1ЦМ и приборах ПКЦ-1111, ПКД-1115 (ЗАО «НПП «Автоматика», г. Владимир), применённых в АСУ ТП«ПХВ-1».

4. Экспериментально подтверждена эффективность разработанных алгоритмов для повышения защищённости узлов сети.

5. Предложено применение программно-аппаратурных имитаторов на базе контроллеров исследуемой АСУ ТП для имитации нештатных ситуаций, в том числе НСД и защитных мероприятий.

6. Разработаны рекомендации по модернизации СЗИ АСУ ТП «ПХВ-1» на основе имитационного моделирования.

7. Разработана методика оценки защищённости АСУ ТП, включающая в себя выбор и обоснование методов определения важности требований, предъявляемых к СЗИ, выбор рационального варианта СЗИ из нескольких возможных. Обоснован показатель качества СЗИ АСУ ТП - уменьшение общего ущерба, наносимого воздействием угроз.

8. Проведена оценка СЗИ АСУ ТП «ПХВ-1» согласно разработанной методике, выбран наилучший вариант СЗИ.

9. Методика построения СЗИ телекоммуникаций АСУ ТП, рекомендации по выбору защищенных программных и аппаратурных средств АСУ ТП, методика оценки информационной защищенности АСУ ТП реализованы в НПО «РИК» (г. Владимир), ООО «Электроприбор» (г. Москва), ООО «ПСВ-Холдинг» (г. Электросталь), ООО «Теза-сервис» (г. Владимир). Внедрение результатов исследований подтверждено соответствующими документами.

10. Содержание работы изложено 8 статьях и трудах НТК. На международных научно-технических конференциях и семинарах сделан 1 доклад.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Казанцев, А. Классификация АСУ ТП [Электронный ресурс]: АСУ ТП и промышленная автоматизация/ А. Казанцев. - Электрон, дан. — М.: Б. и., 2001. — Режим доступа: www.prodcs.ru/ASUTPintro.htm, свободный.

2. Дерябин, А.В. Угрозы информационной безопасности и уязвимости АСУ ТП / А.В. Дерябин, В.М. Дерябин // Проектирование и технология электронных средств. - 2007. - № 1. - С. 47-51.

3. Астахов, А. Особенности обеспечения информационной безопасности промышленных систем/ А. Астахов // CIS A. - 2006. - №3. - С. 76-79.

4. Куприянов, А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений/ А.И. Куприянов, А.В. Сахаров, В.А. Шевцов// - М.: Издательский центр «Академия», 2006. - 256 с.

5. ГОСТ Р 51901-2002. Управление надежностью. Анализ риска технологических систем. - М.: Издательство стандартов, 2002. - 22 с.

6. Галатенко, В.А. Основы информационной безопасности: курс лекций; учеб. Пособие. Издание третье / В.А. Галатенко; под ред. академика РАН В.Б. Бетелина. - М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006. — 208 с.

7. Галкин, А.П. Защита каналов связи предприятий и учреждений от несанкционированного доступа к информации: учеб. пособие / А.П. Галкин. - Владимир: Изд-во ВлГУ, 2003. - 128 с.

8. Хорев, А.А. Методы и средства поиска электронных устройств перехвата информации / А.А. Хорев. - М.: МО РФ, 1998. - 224 с.

9. Расторгуев, С.П. Основы информационной безопасности. Учебное пособие / С.П. Расторгуев. - М.: Academia, 2007. - 192 с.

10. Галатенко, В.А. Стандарты информационной безопасности / В.А. Галатенко; под ред. академика РАН В.Б. Бетелина - М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2004. - 328 с.

11. Казанцев, А. Полевые шины РСУ [Электронный ресурс]: АСУ ТП и промышленная автоматизация / А. Казанцев. - Электрон, дан. - М.: Б. и., 2001. - Режим доступа: www.prodcs.ru/NT_PARTl .htm, свободный.

12. Казанцев, А. Таблица сравнения технических характеристик основных протоколов полевых шин / А. Казанцев. - Электрон, дан. — М.: Б. и., 2001. - Режим доступа: www.prodcs.ru/images/BUSCOMPARE.gif, свободный.

13. Казанцев, А. Промышленные сети верхнего уровня / А. Казанцев. — Электрон. дан. - М.: Б. и., 2001. - Режим доступа: www.prodcs.ru/NT PART2.htm, свободный.

14. Некрасова, Е. Андрей Калашников: «Надо строить безопасные системы, а не системы безопасности» / Е. Некрасова // СЮ. - 2004. - №4. - С. 30-34.

15. Дерябин, А.В. Интеллектуализация датчиков и информационная безопасность / А.В. Дерябин, В.М. Дерябин // Известия института инженерной физики. - 2009. - № 2. - С. 7-12.

16. Дерябин, А.В. Комплексная или поэлементная защита? / А.В. Дерябин, В.М. Дерябин, Тахаан Осама // Перспективные технологии в средствах передачи информации - ПТСПИ-2009: материалы VIII международной научно-технической конференции. - Владимир: Изд-во ВлГУ, 2009. - С. 188.

17. Минтчелл, Гэри А. (Gary A. Mintchell). Средства и системы компьютерной автоматизации. Пришла пора интеллектуальных датчиков / Гэри А. Минтчелл // Control Engineering. - 2002. - №1. - С. 56-59.

18. Ицкович, Э.Л. Современные интеллектуальные датчики общепромышленного назначения, их особенности и достоинства / Э.Л. Ицкович // Датчики и Системы. -2002. - №2. - С. 42.

19. MicroLAN. Новая концепция построения 1 -проводной сети / Фирма Dallas Semiconductor// В кн. Перспективные изделия. - М.: Изд-во ДОДЭКА, 1996. - Выпуск 2. - С. 23-34.

20. Астахов, А. Ключевые угрозы безопасности промышленных систем / А. Астахов // CISA: Открытые системы, 2003. - № 5. - С. 8-11.

21. Полетыкин, А.Г. Концепция обеспечения защиты от несанкционированного доступа АСУ ТП АЭС «Бушер-1» / А.Г. Полетыкин, В.Г. Промыслов, Н.Э. Менгазетдинов // Автоматизация в промышленности. — 2005. - № 5. - С. 3-5.

22. Синк, Перри (Репу Sink). Восемь открытых промышленных сетей и Industrial Ethetrnet / Perry Sink; Synergetic Micro Systems, Inc. // Средства и системы компьютерной автоматизации. — 2002. - № 1. — С. 17-21.

23. Любашин, А.Н. Первое знакомство: краткий обзор промышленных сетей по материалам конференции FieldComms 95 [Электронный ресурс]: Средства и системы компьютерной автоматизации. / А.Н. Любашин. - Электрон, дан. - М.: АО «РТСофт», 1995. - Режим доступа: www.rtsoft.ru, свободный.

24. Иванов, И. Интернет и управление технологическими процессами. / И. Иванов // Средства и системы компьютерной автоматизации. — 2004. — № 2. — С. 23-25.

25. Дерябин, А.В. Эффективность использования GSM канала в системах телекоммуникации АСУ ТП / А.В. Дерябин // Экономический журнал ВлГУ. — Владимир: Изд-во ВлГУ, 2006. - № 6. - С. 12-13.

26. ГОСТ 27.001-95. Межгосударственный стандарт. Система стандартов «Надежность в технике». Основные положения. - Минск: Межгосударственный совет по стандартизации, метрологии и сертификации, 1997. - 3 с.

27. ГОСТ 27.310-95. Межгосударственный стандарт. «Надежность в технике». Анализ видов, последствий и критичности отказов. Основные положения. - М.: Издательство стандартов, 1997. - 12 с.

28. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения. — М.: Издательство стандартов, 1991. — 14 с.

29. ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. - М.: Издательство стандартов, 1991. - 42 с.

30. Нозик, А.А. Автоматизированные системы управления. Надежность и безопасность. Расчет надежности и безопасности автоматизированных систем управления технологическими процессами и инженерным оборудованием. Методические рекомендации / А.А. Нозик, А.С Можаев // СПб.: СПИК СЗМА, 2002. - 34 с.

31. Домарев, В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В.Домарев. - К.: ТИД Диа Софт, 2002. - 688 с.

32. Дерябин, А.В. Методология создания систем защиты АСУ ТП / А.В. Дерябин // Известия института инженерной физики. - 2008. - № 4. - С. 11-14.

33. Программный комплекс автоматизированного моделирования и расчета надежности и безопасности АСУ ТП / А.А. Нозик, А.С. Можаев, С.Н. Потапычев, М.С. Скворцов// В сб.: Материалы III Международной научно-практической конференции, 4.1. - Новочеркасск: ЮРГТУ (БОГЖ), 2003. - С. 8.

34. Новиков, Ю.В., Кондратенко С.В. Основы локальных сетей. Лекция №10: Алгоритмы сети Ethernet/Fast Ethernet / Ю.В. Новиков, С.В. Кондратенко // Интернет-университет информационных технологий. —М.: ИНТУИТ.РУ, 2005. - 360 с.

35. Любашин, А.Н. Профиль PROFIBUS для безопасных систем / А.Н. Любашин // Мир компьютерной автоматизации. - 2000. - №3. - С.33-35.

36. Информационный, измерительный и управляющий комплекс «ДЕКОНТ». Руководство по эксплуатации ДЕПЛ.421457.202РЭ. Часть 1. Техническое описание. - М.: ДЕКОНТ, 2009.

37. Информационный, измерительный и управляющий комплекс «ДЕКОНТ». Руководство по эксплуатации ДЕПЛ.421457.202РЭ. Часть 2. Техническое описание. - М.: ДЕКОНТ, 2009.

38. Информационный, измерительный и управляющий комплекс «ДЕКОНТ». Руководство по эксплуатации ДЕПЛ.421457.202РЭ. Часть 3. Описание

программного обеспечения. -М.: ДЕКОНТ, 2009.

39. Филимонов, Д.А. ТЕКОНИК® - Гибкая система ввода-вывода для построения распределенных систем управления / Д.А Филимонов // Приборы. - 2006. - №9.

40. Интеллектуальный датчик температуры «ТСТ11». Руководство по эксплуатации ДАРЦ.426495.001РЭ. -М.: ЗАО ПК «Промконтроллер», 2007.

41. Преобразователи давления измерительные «ЭЛЕМЕР-АИР-30». Руководство по эксплуатации НКГЖ.406233.007РЭ. - М.: НПП «Элемер», 2008.

42. Прибор для измерений избыточного давления и разрежения воздуха «Ф1791». Руководство по эксплуатации ЗПА.399.156 РЭ. - СПб: ОАО «Приборостроительный завод «ВИБРАТОР», 2007.

43. Прибор одноканальный панельный Ф1775.3-АД. Руководство по эксплуатации ЗПА.399.118 РЭ. - СПб: ОАО «Приборостроительный завод «Вибратор», 2008.

44. Измерители давления многофункциональные «ПРОМА-ИДМ-4х». Руководство по эксплуатации В407.020.000.000-02 РЭ. - Казань: ООО «ПРОМА», 2008.

45. Преобразователь давления Cerabar S. Руководство по эксплуатации ВА 187P/00/ru/04.99. Версия ПО 5.0. Endress+Hauser, 1999.

46. Датчик давления Rosemount 305IS. Руководство по применению 00809-0107-4001. Emerson Process Management, 2002.

47. Преобразователи измерительные Rosemount 644. Руководство по применению 00644-5321-0010. Emerson Process Management, 2003.

48. Датчики давления «Метран-100». Руководство по эксплуатации СПГК.5070.000.00-01 РЭ. Версия 2.4. - Челябинск: МЕТР АН, 2008.

49. Модули измерительные ввода-вывода аналоговых сигналов. Серия NL. NL-8TI, NL-4RTD, NL-8AI. Руководство по эксплуатации. - Таганрог: НИЛ АП, 2007.

50. iTEMP®PA TMT 184 Temperature head transmitter with PROFIBUS-PA® interface. Technical information TI 079R/09/en/02.01 510 03036 FM+SGML

5.5 / HO. Endress+Houser, 2001.

51. JUMO mTRON Communication module. Tyipelist 70.4040. M. K. JUCHHEIM GmbH & Co, Germany.

52. JUMO mTRON Control module. Tyipelist 70.4010. M. K. JUCHHEIM GmbH & Co, Germany.

53. Системное руководство JUMO mTRON. Документация по конфигурированию, установке параметров и инсталляции модулей. Арт. № 70/003343336. JUMO GmbH & Co., Germany.

54. STT 3000 - Series STT250 Smart Temperature Transmitter, Models STT25H, STT25D, STT25M, STT25T. EN1I-6190-A2 6/04. Honeywell International Inc., 2004.

55. Измерительный преобразователь влажности и температуры ДВ2ТС-А. Руководство по эксплуатации. НПК «МИКРОФОР», 2005.

56. JUMO CANtrans T Widerstandsthermometer mit CANopen-Ausgang. Technische Daten. Typenblatt 90.2910. 08.03/00418897. JUMO GmbH & Co. KG, 2003.

57. SIMATIC S7-200 Programmable Controller System Manual. 6ES7298-8FA24-8BH0. Siemens AG, 2008.

58. D-ll-7, D-10-7 Pressure Transmitter with PROFIBUS DP Interface. Operating instructions. 2478159.04 GB/D 06/2007. WIKA Alexander Wiegand GmbH & Co. KG, 2007.

59. D-ll-9, D-10-9 Pressure Transmitter with CANopen Interface. Operating instructions. 2450786.04 GB/D 04/2008. WIKA Alexander Wiegand GmbH & Co. KG, 2008.

60. Датчик дифференциального давления LD 301. Руководство по эксплуатации. BD Sensors. — Чебоксары: Мертек, 2004.

61. Digital Pressure Transducers Specifics Data Series 6000. Operating instructions. CDS6000F. Mensor Corporation, Texas.

62. Преобразователь давления цифровой с интерфейсом RS-485 ПД-1ЦМ. Руководство по эксплуатации АВДП.5070.000.02.РЭ. ЗАО «НПП «Автоматика».

Владимир, 2009.

63. Преобразователь давления цифровой с интерфейсом RS-485 ПД-1ЦМ. Инструкция по настройке АВДП.5070.000.02.ИН. - Владимир: ЗАО «НПП «Автоматика», 2009.

64. Термопреобразователь цифровой с интерфейсом 118-485 ИТ-1ЦМ. Руководство по эксплуатации АВДП.426495.001.02.РЭ. - Владимир: ЗАО «НПП «Автоматика», 2009.

65. Термопреобразователь цифровой с интерфейсом 118-485 ИТ-1ЦМ. Инструкция по настройке АВДП.426495.001.02.ИН. - Владимир: ЗАО «НПП «Автоматика», 2009.

66. Прибор контроля давления ПКД-1115. Руководство по эксплуатации АВДП.406233.115.02.РЭ. - Владимир: ЗАО «НПП «Автоматика», 2008.

67. Прибор контроля давления ПКД-1115. Инструкция по настройке метрологических характеристик АВДП.406233.115.02.ИН. - Владимир: ЗАО «НПП «Автоматика», 2008.

68. Прибор контроля давления ПКД-1115. Коммуникационный интерфейс. Руководство пользователя АВДП.406233.115.02.РП. - Владимир: ЗАО «НПП «Автоматика», 2008.

69. Прибор контроля цифровой с универсальным входом для измерения тока, напряжения, сопротивления и температуры ПКЦ-1111. Руководство по эксплуатации АВДП.399118.111.01.РЭ. - Владимир: ЗАО «НПП «Автоматика», 2009.

70. Прибор контроля цифровой с универсальным входом для измерения тока, напряжения, сопротивления и температуры ПКЦ-1111. Инструкция по настройке метрологических характеристик АВДП.399118.111.01 .ИН. - Владимир: ЗАО «НПП «Автоматика», 2009.

71. Прибор контроля цифровой с универсальным входом для измерения тока, напряжения, сопротивления и температуры ПКЦ-1111. Коммуникационный интерфейс. Руководство пользователя АВДП.399118.111.01.РП. - Владимир: ЗАО «НПП «Автоматика», 2009.

72. Описание программно-технического комплекса «ПХВ-1». 2021.001.ПД.02.2. СВБУ АСУ ТП производства бумвинила. - 2007.

73. Дерябин, А.В. Компоненты и технологии видеонаблюдения / А.В. Дерябин // Современные проблемы экономики и новые технологии исследований: сб. науч. тр., ч. 2 / Филиал ВЗФЭИ в г. Владимире. - Владимир, 2006 - С. 17-21.

74. Information technology — Security techniques — Evaluation Criteria for IT Security. Part 1 : Introduction and general model. ISO/IEC 15408-1:1999.

75. Information technology — Security techniques — Evaluation Criteria for IT Security. Part 2: Security functional requirements. ISO/IEC 15408-2:1999.

76. Information technology — Security techniques — Evaluation Criteria for IT Security. Part 3: Security assurance requirements. ISO/IEC 15408-3:1999.

77. ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель. - М.: Издательство стандартов, 2003. - 12 с.

78. ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности. — М.: Издательство стандартов, 2003.-22 с.

79. ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности. - М.: Издательство стандартов, 2003. - 17 с.

80. Guide for Production of Protection Profiles and Security Targets. ISO/JTC1 /SC27/N2449. DRAFT v0.9, January 2000.

81. Information technology — Security techniques — Protection Profile registration procedures. ISOAEC 15292:2001.

82. Common Evaluation Methodology for Information Technology Security Evaluation. Part 1: Introduction and general model, version 0.6, 19 January 1997.

83. Common Evaluation Methodology for Information Technology Security Evaluation. Part 2: Evaluation Methodology, version 1.0, August 1999.

84. Evaluation Methodology for the Common Criteria for Information Technology Security Evaluation, version 1.1a, 19 April 2002.

85. Руководящий документ — Безопасность информационных технологий — Критерии оценки безопасности информационных технологий — Часть 1: Введение и общая модель. - М.: Гостехкомиссия России, 2002.

86. Руководящий документ — Безопасность информационных технологий — Критерии оценки безопасности информационных технологий — Часть 2: Функциональные требования безопасности. — М.: Гостехкомиссия России, 2002.

87. Руководящий документ — Безопасность информационных технологий — Критерии оценки безопасности информационных технологий — Часть 3: Требования доверия к безопасности. - М.: Гостехкомиссия России, 2002.

88. Руководящий документ — Безопасность информационных технологий — Общая методология оценки безопасности информационных технологий (проект). - М.: Гостехкомиссия России, 2004.

89. Безопасность информационных технологий — Типовая методика оценки безопасности профилей защиты и заданий по безопасности (проект). - М.: Гостехкомиссия России, 2004.

90. Дерябин, А.В. Обеспечение информационной безопасности ИС /А.В. Дерябин // Проектирование и технология электронных средств. - 2008. — № 3. — С. 7-10.

91. Применение алгоритма нечёткого вывода и нечёткой логики в защите информации / А.П. Галкин, А.В. Дерябин, Аль-Муриш Мохаммед, Е.Г. Суслова // Известия института инженерной физики. - 2009. — №2. — С. 13-15.

92. Поспелов, Д.А. Нечеткие множества в моделях управления и искусственного интеллекта / Д.А. Поспелов. - М.: Наука, 1986. - 312 с.

93. Обработка нечеткой информации в системах принятия решений /А.Н. Борисов и др. - М.: Радио и связь, 1989. - 304 с.

94. Ротштейн А.П. Интеллектуальные технологии идентификации / А.П. Ротштейн. - Винница: Универсум-Винница, 1999. - 320 с.

95. Литвак Б.Г. Экспертная информация: методы получения и анализа / Б.Г. Литвак. - М.: Радио и связь, 1982. - 184 с.

96. Заде JI. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. Заде. - М.: МИР, 1976. - 165 с.

97. Гуткин Л.С. Оптимизация радиоэлектронных устройств по совокупности показателей качества / Л.С. Гуткин. - М.: Радио, 1975. - 367 с.

98. Методы определения коэффициентов важности критериев / А.М. Анохин, В.А. Глотов, В.В. Павельев, А.М. Черкашин // Автоматика и телемеханика. - 1997. - №8. - С. 3-35.

99. Wei T.H. The algebraic foundations of ranking theory Theses, Cambridge, 1952.

100. Saaty Thomas L Eigenweinghtor an logarithmic lease sguares // Eur. J. Oper. res, 1990, V. 48, № 1, p. 156-160.

101. Cogger K.O., Yu P. L. Eigenweight vector and least-distance approximation // J. Optimiz. Theory and Appl, 1985, V. 46, №4, p. 483-491.

102. Studler Josef, Weights Search by the Marquardt method // Econ. Math. Obs, 1975, v.21, № 2, p.185-195.

103. Тинтарев, Э.М. Аппроксимация коэффициентов важности функциями ранжирования / Э.М. Тинтарев, В.М. Трофимов // Экономика и мат. методы. - 1975. -Т.П. -№7.~ С. 17-20.

104. Churchmen C.W., Ackoff R. An approximate Measure of Value // Operations Research, 1954, №2, p. 172-181.

105. Подиновский, В.В. Лексикографические задачи линейного программирования / В.В. Подиновский // Журн. вычисл. матем. и мат. физики. - 1972. - Т. 12. -№6. - С. 568-571.

106. Кини, Р.Л. Принятие решений при многих критериях предпочтения и замещения / Р.Л. Кини // - М.; Радио и связь, 1981. - 342 с.

107. Фарберов, Д.С. Сравнение некоторых методов решения многокритериальных задач линейного программирования / Д.С. Фарберов, С.Г. Алексеев // Журнал высш. математики и мат. физики. - 1974. - Т. 14. - №6. - С. 178-180.

108. Метод определения коэффициентов относительной важности / В.А. Глотов и др. // Приборы и системы управления. — 1976. — №8. - С. 17-22.

109. Rosner B.S. A new scaling technique for absolute judgement // Psychometri- ca, 1956, V. 21, №4.

110. Сваровский, С.Т. Аппроксимация функций принадлежности значений лингвистической переменной / С.Т. Сваровский // Математические вопросы анализа данных. - Новосибирск: ВЦ СО АН СССР, 1980. - С. 127-131.

111. Кузьмин, В.Б. Параметрическое отношение лингвистических значений переменных и ограничений / В.Б. Кузьмин // Модели выбора альтернатив в нечеткой среде. - Рига: Б. и., 1980. - С. 75-76.

112. Саати, Т. Аналитическое планирование. Организация систем / Т. Саати, К. Керне. - М.: Радио и связь, 1991. - 224 с.

113. Мулен, Э. Кооперативное принятие решений: аксиомы и модели / Э. Мулен. -М.: Мир, 1991.-463 с.

114. Панкова, Л.А. Организация экспертизы и анализ экспертной информации / Л.А. Панкова, А.М. Петровский, Н.В. Шнейдерман. - М.: Наука, 1984. - 214 с.

Безопасность в АСУ ТП химической промышленности

Пример АСУТП	ЛВС верхнего уровня. ПО верхнего уровня (SCADA)	ЛВС нижнего уровня (Протокол, ПО, интерфейс)	Аппаратура (УСО, контроллеры и тп)	Меры зашиты информации в ЛВС нижнего уровня (физические, программные, аппаратные)	Меры защиты информации в аппаратуре	Меры защиты информации в ПО (БСАРА) и ЛВС верхнего уровня
I	2	3	4	5	б	7

Универсальный программно-технический комплекс для АСУТП химводоподготовкн на Южноуральской ГРЭС (А Решетов, Б Лопаткин, А Елов, СТА 2001, с 60)	Протокол ЛВС: Ethernet IIO: GENHSIS32 v 6.0 компании Iconics Оператор скис станции: IBM PC-совместимый ПК, Pcntium-III 733 МГц Операционная среда Windows NT 4.0.	Протокол ЛВС: МойЬий 1ГШ ПО: БоАВазю фирмы «Прософт-Е» Интерфейс: 118-485	Контроллеры: Advantech PCA-6168F, УСО: Fastwcl UNI096-5, Grayhill 70G, 73G,	1. Возможность размещения аппаратуры вблизи объекта (пыле брызгозашита, виброирочность, широкий температурный диапазон работы, электромагнитная устойчивость) Позволила сократить длину и количество кабелей 2. В N^1)115 данные (кадр) защищаются 16-битным СЯС- кодом	1. Мощность контроллеров позволяет им продолжать работу, в том числе регулирование и защитные функции, при неисправности другого оборудования ПТК или нарушения связи между ними При длительном отсутствии связи между узлами ПТК, например, при отказе пульта управления, может быть произведен автоматический перевод объекта автоматизации в безопасное состояние (можно запрограммировать). 2 Заппсь в энергонезависимое ОЗУ контроллера в конце каждого цикла полной информации о текущем состоянии системы (всс значения переменных, список и состояние запущенных задач и т д) н восстановление этой информации при очередной загрузке контроллера, например, после сбоев энергопитания или срабатывания сторожевого таймера. 3. В энергонезависимом ОЗУ контроллера ведется собственный архив событий с фиксацией даты и времени возникновения события, кода события, необходимой вспомогательной информации, с возможностью просмотра этого архива на дисплее контроллера или средствами верхнего уровня.	1. Обеспечение ограничения доступа (уровня допуска) пользователя к управлению отдельными технологическими операциями, например,изменение параметров регуляторов, 2. Для предотвращения ошибочных действий оператора по управлению оборудованием в дистанционном режиме производится автоматическая блокировка соответствующих виртуальных кнопок на мнемосхеме с выдачей информации о причине запрета этого действия Например, команда оператора на включение насоса блокируется при - отсутствии достоверной информации о состоянии насоса или после аварийного отключения насоса до снятия аварийных признаков оператором; - отсутствии готовности насоса; - малом давлении на входе насоса; - открытой задвижке на выходе насоса; - отсутствии готовности задвижки на выходе насоса; - малом или высоком уровне жидкости в соответствующей емкости. 3. Циклическая архивация входных и выходных параметров, а также событий. 4. Реализация функции «Помощь», предназначенной для облегчения обучения оператора управлению тех процессом и работе с системой
1	*2*	3	4	5	6	7
ЛСУТП стекловаренной печи г. Кингисепп, Ленинградская область (С сайга Сименс-Россня: www.sms-automation ru /projects/ encrgetics/O php)	Протокол ЛВС: Industrial Ethernet ПО: WinCC 5.1 компании SIEMENS Оператор скис станции: (АРМ оператора и АРМ технолога) IBM PC-совмсстимые ПК, Операционная среда Windows	Протокол: РгоПЬиз ОР ПО: Реализуется средствами БСАОА системы Интерфейс:	Основной контроллер: 81МАТ1С 87 400, обеспечивают ий все функции АСУТП, Резервный контроллер: 51МАТ1С Б7-300 УСО: Программус мые регуляторы ЭШАЯТ ОК24.	1. Применение пыле- брызго-защищенных промышленных контроллеров и УСО SIEMENS. 2 В Profibus DP данные защищены 16-битным CRC-кодом	1. Использование основного контроллера для штатного режима работы и переключение на резервный контроллер в случае нештатной ситуации.	1. Архивирование всех параметров технологического процесса и хранение архивов в течение всего срока службы печи (5 лет). 2. Визуализация архивов в виде графиков и формирование отчетов в виде таблиц усредненных значений параметров за каждые полчаса за любую смену в течение всего срока жизни печи. 3. Автоматическая диагностика ПТК. 4. «Безударный» переход в ручной режим управления н обратно. 5 Использование кольцевой резервированной топологии сстн ШщШа) ЕШегпе!
АСУТП химического производства "Аммофос". ОАО "Воскресенские минеральные удобрения" г. Воскресенск (С сайта компании АдАстра \wuv.adastra ги/ apps/cliA mu!)	Протокол ЛВС: Ethernet ПО: TRACE MODE компании Adastra Оператор скис станции: IBM PC-совмсстнмые ПК, Операционная среда Windows	Протокол: МоЛЬиз ЯТи НО: Реализуется средствами 5САРА системы Интерфейс:	Контроллеры: МФК, ТКМ52 ЗАО "ТЕКОН" (г. Москва) в шкафах СМ 1634 УСО: Высоконадежн ыс УСО ЗАО "ТЕКОН" (г. Москва)	1. Применение специальных высоконадежных пыле- брызго-зашшщенных промышленных контроллеров и УСО МФК, ТКМ52 фирмы ЗАО "ТЕКОН". *2* Применение промышленных шкафов СМ1634. 3. Использование промыштенного протокола Modbus, в котором данные защищены 1б-битным CRC-кодом	1. Электропитание контроллеров и ПЭВМ от источников бесперебойного питания *2* Автоматическое, дублированное резервирование контроллеров. 3. Экономичное троированное резервирование операторских станций. 4 Периодическое сохранение производствсшюП информации. 5. Аппаратная и встроенная в программное обеспечение система диагностики работоспособности основных функций, в том числе контроля загруженности сетевого трафика	1 Зашита локальной сстн от хакерских а гак брандмауэром, фильтром-экраном между локальной и корпоративной сетями. 2. Разбиение локальной сети на изолированные сс(менты (подсети). 3. Системное администрирование, направленное на проведение политики безопасности 4 Архивированием учетной информации и копий проектов программного обеспечения. 5. «Безударный» переход в ручной

				\	6. Использованы три многофункциональных контроллера МФК компании "Текон", работающих под управлением Микро МРВ TRACE MODE Два контроллера постоянно эксплуатируются в системе, а третий находится в состоянии "холодного" резерва 7 Схемы протнвоаварийной зашиты, световой и звуковой сигнализации	режим управления и обратно

1	2	3	4	5	6	7
АСУТП энергоблока 200МВт ТЭС Новосибирская ТЭЦ-5 (ОАО "Новосибирскэнерго") (С сайта компании Wonderwarc www.intouch.ru/ projccts/ tec5_6.shtm)	**Протокол** ЛВС: FastEthernet **ПО:** InTouch компании Wonderware Операторские **станции:** IBM PC-совместнмые ПК, Операционная среда Windows (Три операторские станции, образующих 6-и мошлорный АРМ машиниста)	**Протокол:** Ethernet (TCP/IP), **CAN-**BUS **ПО:** ПТК «Торнадо-М» **Интерфейс:**	Контроллеры: новой серии MIF-оснащенные коммуникационными модулями MIF-PPC на базе супсрскалярного oRISC процессора PowerPC, обладающего высокой производительностью около 100 MIPS, встроенным коммуникационным сопроцессором PowerQUlCC. ' Контроллеры установлены в шкафах двухстороннего обслуживания.	1. Контроллеры объединены дублированной сетью Ethernet-100, общей для верхнего и нижнего уровней ПТК. 4. Для связи между контроллерными модулями в пределах одного контроллера и между крейтами, принадлежащими одному контроллеру, используется дублированная сеть CAN-bus, обеспечивающая возможность «горячей» замены модулей без отключения питания контроллера.	**1.** Дублированный сервер базы данных. 2. Дублированный сервер приложений. **3.** Отдельный вспомогательный сервер, обслуживающий принтеры. 4. Предусмотрено внешнее резервирование путем создания отдельной, независимой резервной системы управления. Резервная система обеспечивает безаварийный останов энергоблока в случае отказа основной системы управления. 5. Контроллеры установлены в шкафах со степенью зашиты от внешних воздействий 1Р55. 6. Выносные УСО - в уплотненных шкафах со степенью защиты 1Р55.	**1.** Применена дублированная радиальная топология сети Ethernet системы управления. 2. Разбиение локальной сети на изолированные сегменты (подсети) верхнего и нижнего уровней управления. **3.** В качестве среды передачи данных использовало оптоволокно и витая пара промышленного исполнения.
АСУ ТП наливной эстакады завода окиси этилена АО "Нижнекамск нефтехим" (С сайта НПФ «Круг» \v\vw.krug2000.ru/ solutions/ nizhnekamsk.htm)	**Протокол ЛВС:** Ethernet **ПО:** КРУГ-2000 компании ППФ «Круг» **Операторские станции:** IBM PC-совместимые ПК I LF\, Операционная среда Windows	**Протокол:** Ethernet IEEE 802.3 (TCPJIP) **ПО:** Операционная система-QNX **Интерфейс:** ISA, TREI-5B, RS-232, RS-485	**Контроллеры:** ТРЕЙ-05В **УСО:** Микроконтроллер MTL-I Монтажный **шкаф:** "RITALL"	1. Применение высоконадежных контроллеров - время наработки на отказ - 75 000 часов. 2. Встроенные средства защиты информации протокола TCP/IP	1. Система бесперебойного питания. 2. Автоматический перезапуск контроллеров. 3. Энергонезависимое ОЗУ. 4. Взрывозащпщенное исполнение контроллеров. 5. Контроллеры устанавливаются в термостатический обогреваемый корпус.	1. Управляющие воздействия и изменения логических состояний регистрируются в "Протоколе событий". 2. Тестирование и самодиагностика комплекса технических средств ПТК системы. 3. Подробная экранная помощь. 4. Коррекция системного времени. 5. Автодиагностика состояния сети.

ON

1	2	3	4	5	6	7
АСУТП установок ИКМ и ИМ-1 для контроля антиокислительных и моющих свойств моторных масел (С сайта «ИнСат» www.insat.ru/ projects/ Control_Process _Systems/ petrochemistry/ vnii_np/)	**Протокол JIBC:** Ethernet **ПО:** Master SCADA компании ЗАО «ИНСАТ». **Оператор скне** **станции:** IBM PC-совместимые ПК, Операшюнная среда Windows	**Протокол:** Modbus **ПО:** Реализуется средствами 5САОА системы **Интерфейс:** ЯБ-485	**Контроллеры:** плк 100 к.м фирмы «Овен» **УСО:** МВУ-8, ИП-320, -202 фирмы «Овен»	1. Использование промышленных контроллеров, соответствующих требованиям взрывобезопасности. 2. Использование промышленного протокола Modbus, в котором данные защищены 16-битным СЯС-кодом.	1 Тревожная сигнализация о недопустимом снижении уровня охлаждающей жидкости. 2 Вместо использования лишних проводов и внешних кнопок оператор управляет процессом, нажимая на клавиши ИП-320. При этом все сигналы от ПЛК к панели и обратно пересылаются по одной витой паре	1. Архивирование событий, ведение протокола. 2. Дублированная сеть Ethernet верхнего уровня.
ЛСУТП процесса получения естественных композиционных материалов для газотурбинных двигателей (С сайта компании «PLC-Systems» www.plcsystems .ru/ article/ detail.php? ID=**I** 7262)	**Протокол** ЛВС: Industrial Ethernet **ПО:** Clear SCADA компании Control Microsystems **Операторские** станции: IBM PC-совместимые ПК, Операционная среда Windows	**Протокол:** Modbus **ПО:** Реализуется средствами БСАОЛ системы **Интерфейс:** ЯБ-485	**Контроллеры:** ПЛК DL-205 компании Koyo Inc. **УСО:**	1. Использование промышленныч контроллеров, соогветств}юших требованиям взрывобезопасности 2. Использование промышленного протокола Modbus. в котором данные защищены 16-битным СЯС-кодом.	1 Использование промышленного компьютера с сенсорным монитором в качестве операторской станции 2 Диагностика ошибок встроенными средствами ПЛК' Каждый сигнал подвергается стандартной математической обработке: контроль на достоверность, масштабирование, выбраковка ложных измерений. 3 Защитное отключение нагрузки при превышении тока.	I. «Безударный» переход в режим «ручное управление» обеспечивает завершение автоматизированного цикла в сл>чае его сбоя. 2. При возникновении ошибки на мониторе компьютера появляется окно, в котором отображается код ошибки, описание ошибки, рекомендации оператору. 3. Применение защищенного протокола Industrial Ethernet в сетях верхнего уровня.

−С

1	2	3	4	5	6	7
АСУТП установки легкого гидрокрекинга Л-24/8С на ОАО «Сызранский НПЗ» (С сайта «Инкомсистем» www.incomsystem.ru/ application/)	**Протокол ЛВС:** Industrial Ethernet **ПО:** DeltaV компании EMERSON Process Management (Fisher-Rosemount).	**Протокол:** Modbus **ПО:** Реализуется средствами SCADA системы **Интерфейс:** RS-485	**Контроллеры:** M5+ Modicon TSX Quantum фирмы Schneider Electric **УСО:** искробезопасн ые 8-канальные модули	1. Использование промышленных контроллеров, соответствующих требованиям взрывобезопасности. 2. Применение искробезопасных УСО **3.** Использование промышленного протокола МоёЬи5, в котором данные защищены 16-битным CRC-кодом.	1. Для повышения надежности выполнено резервирование контроллеров. 2. Отдельная программно-аппаратная система противоаварийной защиты. **3.** Резервированные источники питания.	1. ПО включает в себя систему сигнализации нарушений и включает в себя средства защиты от несанкционированного доступа к функциям системы. 2. Применение резервированной сети Ethernet

	Оператор скне станции: IBM PC-совместимые ПК, Операционная среда Windows NT		аналогового ввода/вывода, 32-канальные модули дискретного ввода/вывода, интерфейсный модуль для связи с системой ПАЗ. **Монтажные шкафы:** "RITALL"			

(Л
оо

Безопасность в 8САОА/НМ1-Системах

	Б1МАТ1С \ VINCC ^¡етепз, Германия)	ТЯАСЕ МОРЕ 6 (Ас^га, Россия)	ОЕЫЕ31832 Осошсэ, США)	1ытоисн (\Vonderware, США)	СГГЕСТ (Скей, США)	КРУГ- 2000 («НПФ Круп», Россия)	КеаИех (Кса1Псх ТесЬпо^ез , Ирландия)	Ма51ег5САО А (ЗАО «ИнСАТ», Россия)	аеагБСАОА (СоШго! Мкгс^штз , Канада)	¡Р1Х (6Е РАЬИиС, США, Япония)	ЮББ (Беуеп ТесЬпо1о§1ез , Дания)	ОрепБСАОА (Нсхависимыс разработчики, старт - Украина)
Ведение архива событии	+	+	+	+	+	+	+	+	+	+	+	+
Защита настроек паролем	+	+	+	+	+	+	+	+	+	+	+	+
Разграничение прав доступа пользователей	+	+	+	+	+	+	+	+	+	+	+	+
Настройка разрешенного времени для входа пользователя	+	+	+	+	+	+	+ .	+	+	+	+	–
Горячее резервирование	+	+	+	+	+	+	+	+	+	+	+	+
Удаленная перезагрузка конторллеров	+	+	+	+	+	+	+	+	+	+	+	–
Синхронизация системного времени	+	+	+	+	+	+	+	+	+	+	+	+
Самотестирование, обнаружение ошибок	+	+	+	+	+	+	+	+	+	+	+	+
Уведомление тревоге на экране	+	+	+	+	+	+	+	+	+	+	+	+

Уведомление о тревоге звуковое	+	+	+	+	+	+	+	+	+	+	+	+
Функции сторожевого таймера	+	+	+	+	+	+	+	+	+	+	+	+
Автоматический Старт/Перезагрузк а системы в случае ошибки	+	+	+	+	+	+	+	+	+	+	+	+
Информация об ошибках коммуникации	+	+	+	+	+	+	+	+	+	+	+	+

чэ

	SIMATIC WINCC (Siemens, Германи)	TRACE MODE 6 (Adastra, Россия)	GENESIS32 (Iconics, США)	INTOUCH (Wonderware, США)	CITECT (Citect, США)	КРУГ-2000 («НПФ Круг», Россия)	RealFlex (RealFlex Technologies , Ирландия)	MasterSCAD A (ЗАО «ИнСАТ», Россия)	CtearSCADA (Control Microsystems , Канада)	¡FIX (GE FANUC, США, Япония)	IGSS (Seven Technologies , Дания)	ОрепвСАЛА (Нехависимые разработчики, старт -Украина)
Автоматический контроль свободной памяти диска	+	+	+	+	+	+	+	+	+	+	+	–
Восстановление исходных настроек параметров	+	+	+	+	+	+	+	+	+	+	+	+
Контроль достоверности параметров измерения	+	+	+	+	+	+	+	+	+	+	+	+
Контроль допустимости вводимой оператором информации	+	+	+	+	+	+	+	+	+	+	+	+
Блокировка определенных команд в аварийной ситуации	+	+	+	+	+	+	+	+	+	+	+	+
Контекстная помощь к управлению	+	+	+	+	+	+	+	+	+	+	+	–
Интуитивный графический НМ1-интерфейс	+	+	+	+	+	+	+	+	+	+	+	+

О
–

i

o

	SIMATIC WINCC (Siemens, Германи)	TRACE MODE 6 (Adastra, Россия)	GENESIS32 (Iconics, США)	INTOUCH (Wondcrware, США)	CITECT (Citect, США)	КРУГ-2000 («НПФ Круг», Россия)	RealFlex (RealFlex Technologies, Ирланди я)	MasterSCAD A (ЗАО «ИнСАТ», Россия)	ClearSCADA (Control Microsystems , Канада)	¡P1X (вЕ FANUC, США, Япония)	IGSS (Seven Technologies , Дания)	OpenSCADA (Нехависимые разработчики, старт -Украина)
Соответствие ПО стандартам безопасности	+ ISO 9001; IEC 61508; DIN V 19250; DIN V 19251; EN 60204-1; EN 954-1;	+ ISO 9001; IEC 61131-3; Сертифик ация в соответств ии с требовани ями FDA, 21 CFRI1;	+ Сертификаци я в соответствии с требованиями FDA, 21 CFR И;	+ Сертификаци я в соответствии с требованиями FDA, 21 CFR п;	+ ISO 9001; Сертификаци я в соответствии с требованиями FDA, 21 CFR И;	+ ГОСТ 24. 104-85; ГОСТ 12.2.007-075; ГОСТ 12.2.003-74; ГОСТ 12.3.002-75	+ ISO 9001;	+ ISO 9001; ГОСТ	+ ISO 9001; IEC 61131-3; EN 61000-64; EN 55022; EN 61000-62; EN 500821	+ 150 9001; а также основные мировые стандарты и стандарты Евросоюз а	+ ISO 9000;	+ Не сертифицируете я
Переемственность версий программного обеспечения	+	+	+	+	+	+	+	+	+	+	+	-
Гарантированная техническая поддержка разработчика	+	+	+	+	+	+	+	+	+	+	+	-
Гибкость. Взаимодействие с другими программными средствами с помощью технологий OPC, ODBC, DCOM, OLE, OLEDB, ActiveX, ODBC...	+	+	+	+	+	+	+	+	+	+	+	+/- (ОС Linux)
Беспроводные коммуникационны е протоколы	+	+	+	+	+	+	+	+	+	+	+	+
Проводные коммуникационны е протоколы	+	+	+	+	+	+	+	+	+	+	+	+

ПРИЛОЖЕНИЕ 3

Подсистема безопасности в БСАВА-системе ШТ011СН

Интегрированная БСАБА/БМ! система ШТОиСН 9.5 располагает мощной системой безопасности, способной максимально защитить работающую АСУ ТП от несанкционированного доступа и ошибок персонала.

И«* А*>-келщр | Хлсикк

- «1ЙММШ«* - ——

I П*ЙЛ>.....8 -»П I □

, г |

I ¡3 , | О Рвнктчмм»«»

В Осг»ев 11 0

{3 ^ | (3 Умпам

1 1 ГяУЛА --- ~~

> ¡ЗКеигирсм«« ! □ Рвдактнх«^

I
mxm O дс^/к«« Экр-х« □ Умлм»
. ппщрррб ;
л 1

Система безопасности ШТОиСН основана на системе паролей. В инструментальной системе создаются группы пользователей. Число групп не ограничивается. В каждой группе может быть произвольное количество пользователей АСУ ТП. Деление на группы условно и, в принципе, должно соответствовать количеству должностей и рабочих групп, имеющих отношение к данной АСУ.

Каждый пользователь, будь то оператор, технолог, мастер, администратор или директор, обладает своим набором прав доступа к компонентам информационной системы - к экранам, элементам управления и функциям управления. При загрузке АСУ ТП или АСУП система безопасности ШТОиСН проверяет имя и пароль пользователя и предоставляет ему только те права, которыми он обладает. Если пароль введен не будет, то система безопасности не даст АСУ ТП запуститься.

Если необходимо организовать автоматическую загрузку системы, то в ней должен быть прописан пользователь «по умолчанию», обладающий минимальными правами.

Система безопасности ШТОТЛСН контролирует ввод пароля и при выходе пользователя из системы.

Смену пользователя можно производить, не останавливая работу АСУ ТП. Если, например, 8САХ)А-система загружена с правами оператора, то для выполнения функций, технолога (входа в диалог настройки регуляторов) потребуется заново зарегистрироваться в системе под именем и паролем технолога. По окончании настройки регуляторов технолог должен выйти из системы, выбрав в качестве текущего пользователя оператор. Более того, администратор системы может удаленно поменять права пользователя, послав команду через сеть.

Система безопасности ШТОиСН позволяет редактировать список пользователей в реальном времени, добавлять или удалять пользователей , не прерывая работы АСУ ТП. Доступ к АСУ ТП протоколируется системой безопасности ГЫТОиСН в отчет тревог, что позволяет при необходимости восстановить хронологию событий и действий персонала.

В случае, если сервер ГМТОиСН имеет выход в интернет или интранет, может встать вопрос защиты файла проекта, содержащего коммерческую информацию. На этот случай существует возможность заказа индивидуальной линии ключей ЮТОИСН, несовместимых с обычными ключами по форматам данных проекта.

Разработчик БСАВА-системы: компания «\VonderWare».

Что такое SCADA-системы

Термин SCADA-система используют для обозначения программно-аппаратного комплекса сбора данных (телемеханического комплекса).

К основным задачам, решаемым SCADA-системами, относятся:

- Обмен данными в реальном времени с УСО (устройством связи с контролируемым объектом). Этим устройством может быть как промышленный контроллер, так и плата ввода/вывода.
- Обработка информации в реальном времени.
- Отображение информации на экране монитора в понятной для человека форме (HMI сокр. от англ. Human Machine Interface — человеко-машинный интерфейс).
- Ведение базы данных реального времени с технологической информацией.
- Аварийная сигнализация и управление тревожными сообщениями.
- Подготовка и генерирование отчетов о ходе технологического процесса.
- Архивирование технологической информации (сбор истории).
- Обеспечение связи с внешними приложениями (СУБД, электронными таблицами, текстовыми процессорами и т.д.). В системе

управления предприятием такими приложениями чаще всего являются приложения, относимые к уровню MES.

Иногда SCADA-системы комплектуются дополнительным ПО для программирования промышленных контроллеров. Такие SCADA-системы называются интегрированными, и к ним добавляют термин SoftLogic.

Это была сухая формулировка, взятая из энциклопедии. На самом деле системы такого класса имеют четкое предназначение — они предоставляют возможность осуществлять мониторинг и диспетчерский контроль множества удаленных объектов (от 1 до 10000 пунктов контроля, иногда на расстоянии в тысячи километров друг от друга) или одного территориально распределенного объекта. Классическими примерами являются:

- Нефтепроводы;
- Газопроводы;
- Водопроводы;
- Удалённые электрораспределительные подстанции;
- Водозаборы;
- Дизель-генераторные пункты и т.д.

Основная задача БСАЭА — это сбор информации о множестве удаленных объектов, поступающей с пунктов контроля, и отображение этой информации в едином диспетчерском центре. Кроме этого, 8САХ)А должна обеспечивать долгосрочное архивирование полученных данных. При этом диспетчер зачастую имеет возможность не только пассивно наблюдать за объектом, но и ограниченно им управлять, реагируя на различные ситуации.

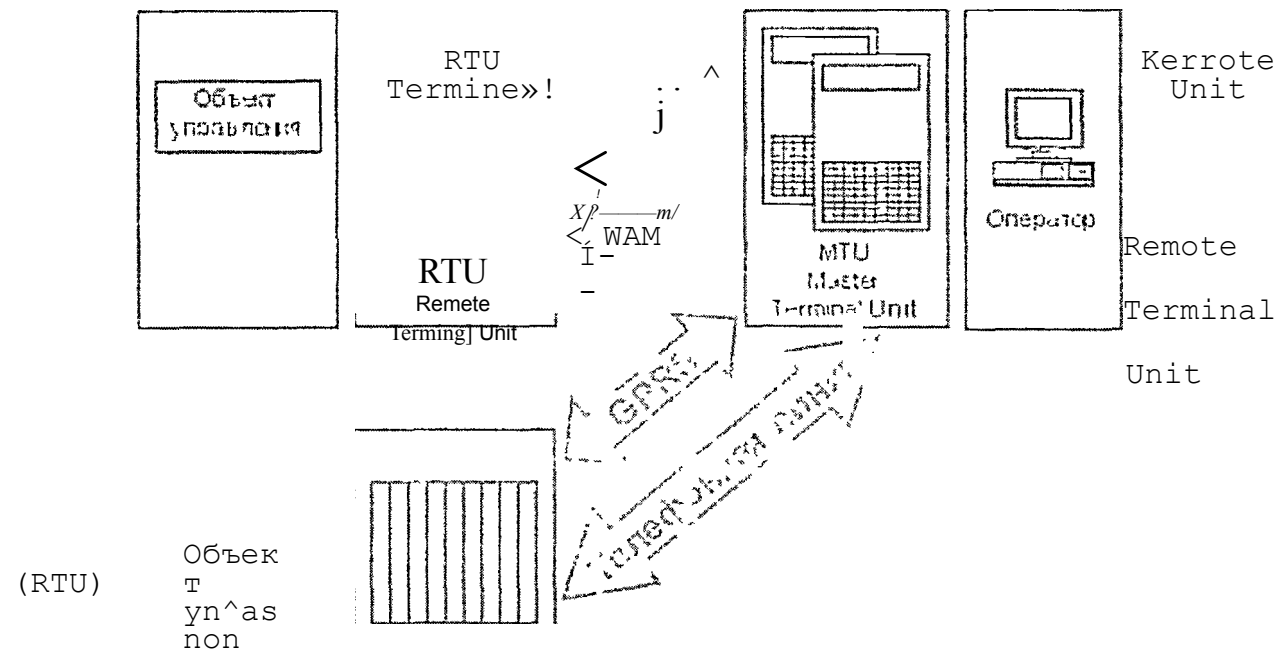
Общая структура вСАБА

Работа БСАОА - это непрерывный процесс сбора информации реального времени с удаленных точек (объектов) для обработки, анализа и возможного управления.

Требование обработки реального времени обусловлено необходимостью оперативной доставки (выдачи) всех сообщений и данных на центральный

интерфейс оператора (диспетчера). В то же время понятие реального времени отличается для различных 8САБА-систем.

Все современные ЗСАЭА-системы включают три основных структурных компонента (см. рисунок ниже):



(RTU) Объект yn^as non

удаленный терминал, подключающийся непосредственно к контролируемому объекту и осуществляющий обработку задачи (управление) в режиме реального времени. Спектр воплощений RTU широк: от примитивных датчиков, осуществляющих съем информации с объекта, до специализированных многопроцессорных отказоустойчивых вычислительных комплексов, осуществляющих обработку информации и управление в режиме жесткого реального времени. Конкретная его реализация определяется спецификой применения. Использование устройств низкоуровневой обработки информации позволяет снизить требования к пропускной способности каналов связи с центральным диспетчерским пунктом.

Master Terminal Unit (MTU), Master Station (MS) диспетчерский пункт управления (главный терминал); осуществляет обработку данных и управление высокого уровня, как правило, в режиме мягкого (квази-) реального времени. Одна из основных функций - обеспечение человеко- машинного интерфейса (между человеком-оператором и системой).

В

зависимости от конкретной системы MTU может быть реализован в самом разнообразном виде: от одиночного компьютера с дополнительными устройствами подключения к каналам связи до

больших вычислительных систем (мэйнфреймов) и/или объединенных в локальную сеть рабочих станций и серверов. Как правило, и при построении MTU используются различные методы повышения надежности и безопасности работы системы. Устройство MTU часто называют SCADA-сервером.

Communication System (CS) коммуникационная система (каналы связи) между RTU и MTU. Она необходима для передачи данных с удаленных точек (RTU) на центральный интерфейс диспетчера и передачи сигналов управления обратно с MTU на RTU. В качестве коммуникационной системы можно использовать следующие каналы передачи данных:

- Выделенные линии - собственные или арендованные; медный кабель или оптоволокно;
- Частные радиосети;
- Аналоговые телефонные линии;
- Цифровые ISDN сети;
- Сотовые сети GSM (GPRS).

С целью дублирования линий связи устройства могут подключаться к нескольким сетям, например к выделенной линии и резервному радиоканалу.

Особенности SCADA как процесса управления

Ниже перечисленные некоторые характерные особенности процесса управления в современных диспетчерских системах:

- В системах SCADA обязательно наличие человека (оператора, диспетчера);
- Любое неправильное воздействие может привести к отказу (потере) объекта управления или даже катастрофическим последствиям;

- Диспетчер несет, как правило, общую ответственность за управление системой, которая, при нормальных условиях, только

изредка требует подстройки параметров для достижения оптимального функционирования;

- Большую часть времени диспетчер пассивно наблюдает за отображаемой информацией. Активное участие диспетчера в процессе управления происходит нечасто, обычно в случае наступления критических событий - отказов, аварийных и нештатных ситуаций и пр.;
- Действия оператора в критических ситуациях могут быть жестко ограничены по времени (несколькими минутами или даже секундами).

Термины АСУ ТП

АСУ ТП. Автоматизированная система управления технологическим процессом.

ИУ. Исполнительное устройство. Звено в контуре управления, служащее для непосредственного воздействия на объект управления.

ОУ. Объект управления. Звено в контуре управления. В общем смысле для АСУ ТП объектом управления является сам технологический процесс.

САУ. Система автоматического управления.

УУ. Управляющее устройство. Звено, в контуре управления, вырабатывающее для ОУ управляющее воздействие в соответствие с определенными алгоритмами автоматического управления. В простейшем случае - регулятор.

AI (Analogue Input). Ввод аналоговых полевых сигналов.

ALARM. Аварийная сигнализация.

AO (Analogue Output). Вывод аналоговых полевых сигналов.

ARCHIVE (Архив, История). Архив значений технологических параметров за прошедший период времени. Часто еще называется **HISTORICAL ARCHIVE.**

AS (Automation Station). Обобщенное название любого устройства, осуществляющего автоматизированное управление.

BASEPLATE. Базовая панель. Служит для установки электронных модулей в специальные слоты. Неотъемлемая часть модульной системы.

CFC (Continuous Flow Chart). Непрерывная функциональная диаграмма. Язык программирования ПЛК.

DCS (Distributed Control System). Распределенная система управления (РСУ).

DI (Discrete Input). Ввод дискретных полевых сигналов.

DISTRIBUTED IO, REMOTE IO. Распределенный (удаленный) ввод/вывод. Полевой ввод/вывод, расположенный на значительном удалении от центрального устройства управления.

DO (Discrete Output). Вывод дискретных полевых сигналов.

ES (Engineering Station). Инженерная станция. Станция инженерного обслуживания АСУ ТП.

EX (сокр. от слова Explosive). Так обозначаются взрывоопасные зоны и участки производства. Такую маркировку имеет оборудование, предназначенное для эксплуатации во взрывоопасных зонах.

FACEPLATE (Фейсплейт). Дословно "Лицевая панель". Графический элемент человеко-машинного интерфейса, предназначенный для управления технологическим устройством.

FBD (Functional Block Diagram). Диаграмма функциональных блоков. Один из пяти стандартизированных языков программирования ПЛК.

FEEDBACK. Обратная связь. Информационная связь в контуре регулирования между датчиком, измеряющим значение регулируемой

величины, и входом регулятора.

FO (Fiber Optic). Оптоволокно. Физическая среда передачи данных.

HMI (Human Machine Interface). Человеко-машинный интерфейс (ЧМИ). Интерфейс взаимодействия человека-оператора с АСУ ТП.

IL (Instruction List). Список инструкций. Один из пяти стандартизированных языков программирования ПЛК.

INDUSTRIAL ETHERNET. Семейство протоколов промышленных сетей на базе Ethernet (IEEE 802.3). К Industrial Ethernet обычно относят Profinet, EtherCAT, Ether/IP и некоторые другие.

INTERFACE MODULE. Интерфейсный модуль. Электронный модуль для подключения устройства к сети.

IO (Input Output). Подсистема ввода/вывода полевых сигналов. Неотъемлемая часть любой АСУ ТП.

IO BUS. Цифровая шина полевого ввода/вывода. Как правило, связывает контроллер и удаленные устройства ввода/вывода.

IO MODULE. Электронный модуль для подключения полевых приборов: датчиков и исполнительных механизмов. Часть подсистемы ввода/вывода.

IS (Intrinsically Safe). Так обозначаются электрооборудование и электрические цепи, в которых реализована взрывозащита вида «искробезопасная электрическая цепь» (искрозащита).

IS-Barrier (Intrinsically Safe Barrier). Барьер искробезопасности.

IS RIO (Intrinsically Safe Remote Input/Output). Система искробезопасного удаленного ввода/вывода.

LAN (Local Area Network, ЛВС). Локальная вычислительная сеть.

LD (LAD, LADDER). , Лестничная диаграмма. Один из пяти стандартизированных языков программирования ПЛК.

LOCAL IO (Input Output). Локальный ввод/вывод. Ввод/вывод, встроенный непосредственно в устройство управления, либо установленный- на той же базовой панели виде модульной системы.

MASTER. Ведущее устройство на шине передачи данных.

MES (Manufacturing Execution System). Производственная исполнительная система. Комплексное решение для управления производством на уровне завода (фабрики).

MODBUS, PROFIBUS, DEVICENET, CAN, FOUNDATION FIELDBUS (FF). Промышленные стандарты передачи данных по цифровым шинам. Существуют разновидности каждого из этих стандартов.

MTU (Master Terminal Unit). Главный терминал. Компонент SCADA- систем.

NIC (Network Interface Card). Интерфейсная карта для подключения компьютера к сети.

OLM (Optical Link Module). Преобразователь среды передачи данных «оптоволокно-медь».

OPC (OLE for Process Control). Клиент-серверный протокол обмена данными между распределенными приложениями. Применяется в промышленных системах.

OPERATOR PANEL (Операторская Панель). Компактная вычислительная машина со встроенным жидкокристаллическим дисплеем, предназначенная для визуализации и операторского управления технологическим процессом.

OS (Operator Station). Операторская рабочая станция для управления технологическим процессом.

PCS (Process Control System). Автоматизированная система управления технологическим процессом (АСУ ТП).

PID (ПИД, пропорционально-интегро-дифференциальный). Разновидность непрерывного регулятора, применяемого для поддержания заданного значения регулируемой величины.

PLC (Programmable Logic Controller). Программируемый логический контроллер (ПЛК). В узком смысле - аппаратное обеспечение, реализующее- автоматизированное управление технологическим процессом. В широком понимании - класс АСУ ТП.

PV (Process Value). Текущее значение регулируемой величины, подаваемое на вход регулятора. Таким образом реализуется обратная связь.

REDUNDANT PAIR. Резервированная пара. Пара модулей, работающих параллельно и страхующих друг друга. Метод повышения отказоустойчивости системы.

RTU (Remote Terminal Unit). Удаленный терминал. Компонент SCADA-систем.

SCADA (Supervisory Control and Data Acquisition). В узком смысле - пакет визуализации процесса. В широком понимании - класс АСУ ТП.

SCAN CYCLE. Цикл сканирования. Время, за которое контроллер выполняет полный цикл операций.

SERVER. Сервер для обслуживания множества операторских станции и других ПК.

SETPOINT. Уставка, заданное значение регулируемой величины, подаваемое на вход регулятора.

SFC (Sequential Function Chart). Язык последовательных функциональных схем. Один из пяти стандартизированных языков программирования ПЛК.

SLAVE. Ведомое устройство на шине передачи данных.

STP, RSTP (Spanning Tree Protocol, Rapid Spanning Tree Protocol). Протоколы IEEE 802.Id и 802.lw соответственно. Позволяют создавать петлевидные топологии на базе Ethernet.

SPOF (Single Point of Failure). Единичная точка отказа.

ST (Structured Text). Структурированный текст. Один из пяти стандартизированных языков программирования ПЛК.

TERMINAL BUS. Шина передачи данных между операторскими станциями, контроллерами и серверами. Сеть верхнего уровня АСУ ТП.

TREND (Тренд). График изменения параметра (параметров) технологического процесса. Различают тренд реального времени и исторический тренд.

VISUAL SUPERVISOR (Графический Супервизор). Промышленный контроллер со встроенным человеко-машинным интерфейсом.

Условия эксплуатации

По устойчивости к воздействию температуры и влажности окружающего воздуха в процессе эксплуатации по ГОСТ 26.205 оборудование ПТК «ПХВ-1» должно соответствовать категориям, указанным в Таблица 3.1.

Таблица 3.1. Требования к оборудованию ПТК «ПХВ-1» Г руга»	Тпш С	Тпкм -с	Ошоешсяиюя ВЛЯЖИиСТЬ,"'»	1" король нарастдо«	Категория iKiMt.iiv.-i6B! по ГОСТ 26.205 (г^тата)
04	+5		О г 5 до 95 без конденсации ьлаг.1	*20*	Обогреваемые или охлаждаемые помешан я
С4	-30		От 5 до 100 кочдепсзции *1* язи'	10	Под коышей или г ;~.ц>ыты'/поглгшр-т'

Электроснабжение

Основное электропитание шкафов автоматики и фронтальных контроллеров распределенных АСУ ТП осуществляется от сети переменного тока 1 категории напряжением -220В +22/-33В, частотой 50 Гц и от ЩПТ (щит постоянного тока) напряжением постоянного тока =220В +22/-33В (резервное питание).

Для защиты от провалов входного напряжения и нарушения работоспособности питаемого электронного оборудования, основное электропитание локальных и фронтальных контроллеров дублируется от резервного источника питания постоянного тока напряжением =220 В (аккумуляторная батарея).

Для управления ЭПУУ кранов к шкафам автоматики подается питание напряжением постоянного тока =220 В от щита постоянного тока (ЩПТ).

Питание датчиков, подключаемых к шкафам автоматики, осуществляется от источников постоянного тока напряжением =24 В этих шкафов.

Для бесперебойного питания автоматизированного рабочего места сменного инженера (основного и резервного АРМ СИ) применяется источник бесперебойного питания (ИБП) без обслуживания батарейного питания, работающий от цепей переменного тока -220В и внешней аккумуляторной батареи =220 В.

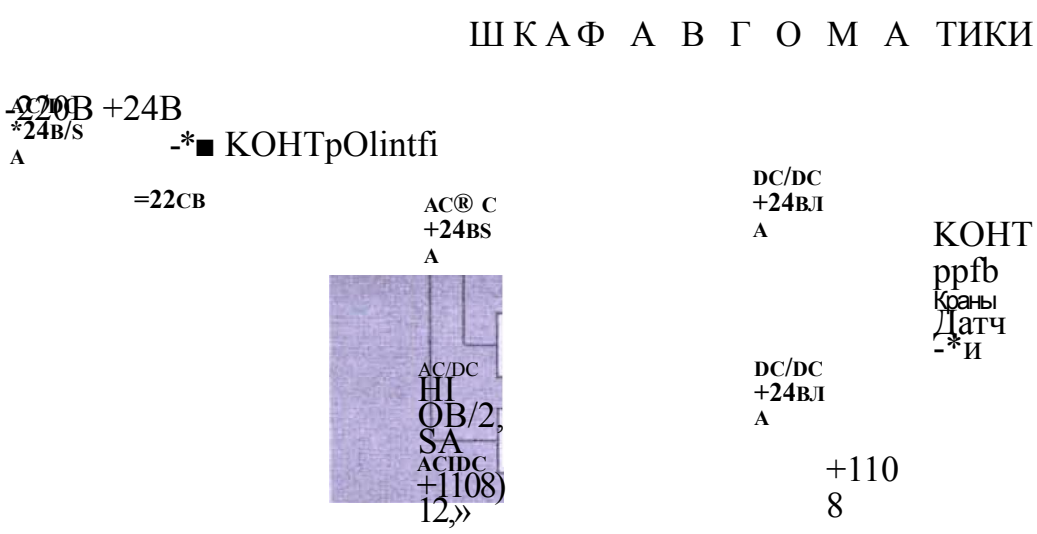
Питание оперативным током вторичных цепей шкафного оборудования ПТК «ПХВ-1» осуществляется через автоматические выключатели с защитой по току.

Устройства релейной защиты, автоматики и управления ответственных элементов имеют постоянно действующий контроль состояния цепей питания -220В и =220В.

Источник питания (ИП) типа «W» (фирма Melcher), мощностью не менее 125 Вт и преобразователи DC/DC типа «ИРБИС», мощностью 25 Вт, применяемые в ПТК «ПХВ-1», удовлетворяют следующим основным требованиям:

- диапазон входных напряжений: -220В +22/-33В; =220В +22/-33В (универсальный вход);
- выходное напряжение: +5В, +12В, +24В;
- PI-фильтр на входе и выходе;
- мощность не менее 30 Вт;
- пульсации на выходе ИП не более 100 мВ;
- работа в резервном режиме;
- индикация питания;
- гальваническая развязка входа/выхода;
- установка выходного напряжения;
- возможность работы без нагрузки, защита от короткого замыкания, перенапряжения на выходе и перегрева;
рабочая температура окружающей среды (25.. .60) °С
.
-

Схема электропитания шкафов автоматики ПТК «ПХВ-1» является распределенной, с резервированием. Типовая схема распределения электропитания в ПТК «ПХВ-1» представлена на Рисунок 3.1 .



АСФС - LWRI401,
LWRJH80 DC.BC’-
F-MPU?5t

Рисунок 3.1. Типовая схема распределения электропитания в НТК «ПХВ-1»

Защитное заземление

Контур защитного заземления ПТК «ПХВ-1» соединяется по типу с глухозаземленной нейтралью для основного оборудования, расположенного на базовой площадке, и по типу с изолированной нейтралью для периферийных площадок. Контур защитного заземления с сопротивлением растеканию тока не более 4 Ом объединяется с рабочим заземлением на уровне распределительных коробок либо составляет общее рабочее заземление.

Типовая схема заземления шкафного оборудования в ПТК «ПХВ-1» представлена на Рисунок 3.2

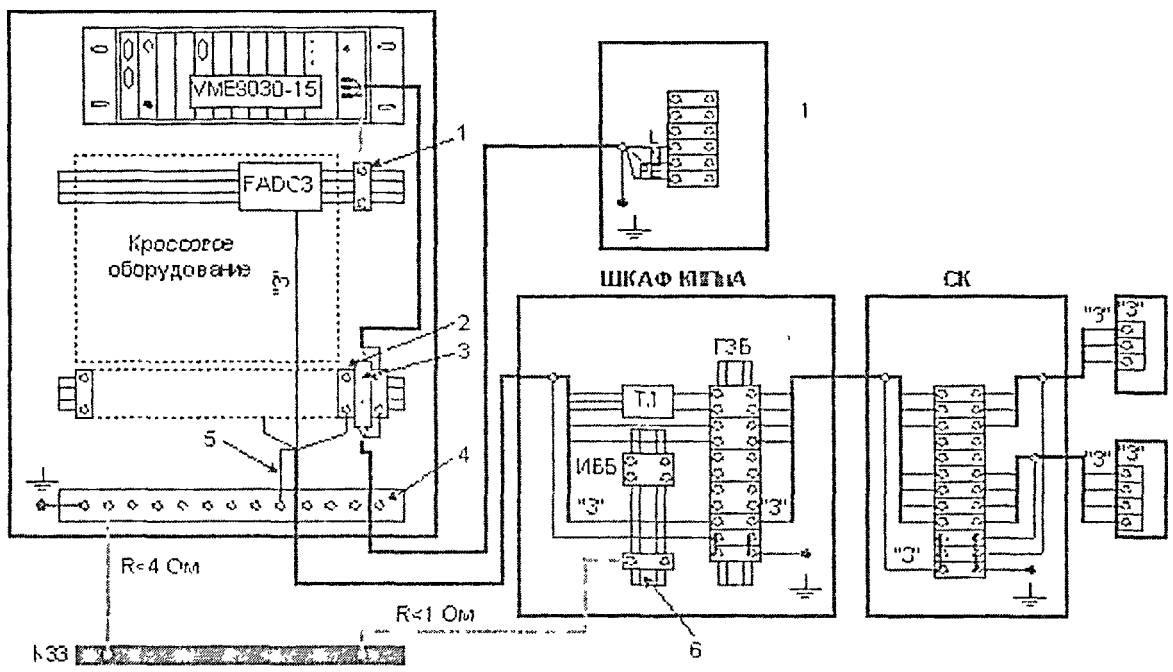
.

Защитные барьеры

Защита цепей питания, измерительных и информационных каналов ПТК «ПХВ-1» от электромагнитных помех, перенапряжений, вторичных проявлений грозовых токов и возникновение искры во взрывоопасной зоне осуществляется защитными барьерами искробезопасности.

Для защиты цепей питания, измерительных и информационных каналов от вторичных воздействий молний в шкафах автоматики применяются грозозащитные барьеры (ГЗБ).

Для защиты измерительных каналов, находящихся во взрывоопасной зоне, применяются датчики во взрывобезопасном исполнении (Exc1), а в шкафах автоматики преобразователи со встроенными искробезопасными барьерами (ИББ).



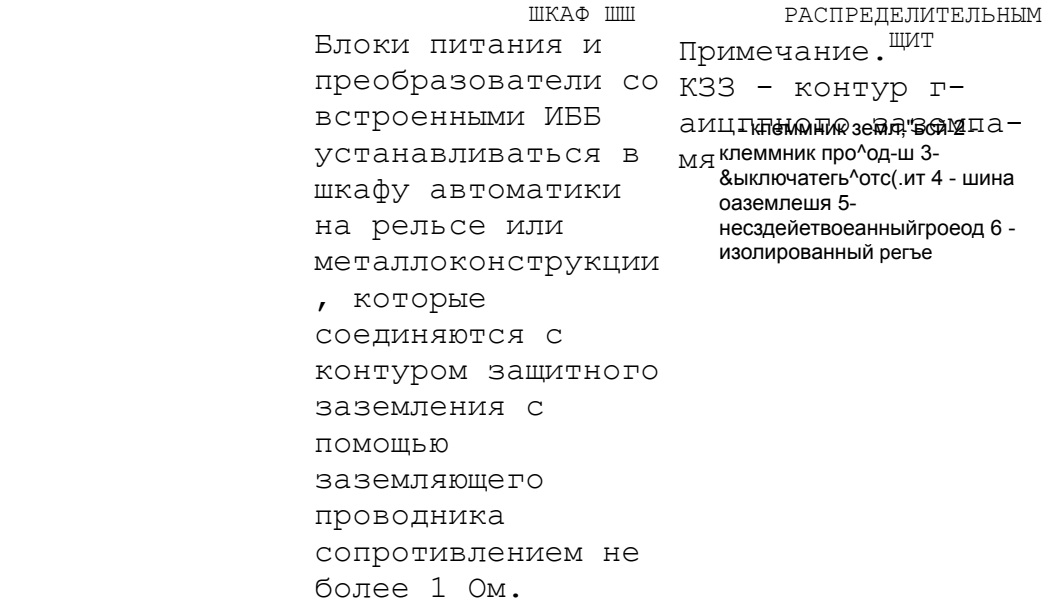


Рисунок 3.2. Пример заземления шкафного оборудования ПТК «ПХВ-1»

На рынке предложений шкафного оборудования высокую конкурентоспособность имеет оборудование фирмы RITTAL.

Шкафы по пылевлагозащищенности соответствует международным стандартам, степень защиты IP54, высокая технологичность при сборке, широкая номенклатура составных частей и принадлежностей.

Шкафы ПТК «ПХВ-1» подразделяются на три типа по функциональному назначению:

- шкаф фронтального

контроллера напольный;

- шкаф автоматики напольный;
- шкаф автоматики настенный.

По конструктивному назначению шкафы ПТК подразделяются на два типа:

- шкаф напольный типа DK7771 фирмы RITTAL;
- шкаф настенный типа AE1260 фирмы RITTAL.

Блок аварийного останова

Система безопасности рабочего персонала и эксплуатационного оборудования распределенных АСУ ТП базируется на применении блока экстренного аварийного останова (БЭАО). БЭАО ПТК «ПХВ-1» является распределенным аппаратным устройством, который включает следующие узлы:

- пульт БЭАО;
- основной управляющий и исполнительный (релейный) узел распределенной схемы БЭАО в шкафу цехового контроллера или отдельном шкафу контроллера БЭАО;
- контроллер БЭАО;
- узел управляющих и исполнительных реле в шкафу локального контроллера узла подключения (УП);
- узел управляющих и исполнительных реле в шкафу локального

контроллера общестанционных замеров и кранов (ОЗК);

- узел управляющих и исполнительных реле в шкафу локального контроллера блока подготовки сырья (БПС);
- кроссовый узел в шкафу локального контроллера аппаратов воздушного охлаждения (АВО);
- кроссовый узел в системе автоматического управления

напыляющими агрегатами САУ НА;

- коммутационные цепи БЭАО.

- БЭАО функционирует в 2-х режимах:

- экстренный аварийный останов цеха, агрегатов, выполняемый аппаратным способом, использующий только физические связи;

- аварийный останов цеха, выполняемый программно-аппаратным способом по алгоритмам с

учетом всех условий и технологических зависимостей.

Аварийный останов инициализируется по команде оператора с пульта БЭАО или АРМ при возникновении аварийных ситуаций, таких как пожар на станции, превышение температуры сырья в котле, выход за пределы уставок на секущем кране, пропадание основного электропитания,

обрыв собственных обеих резервных цепей БЭАО. Исходя из последней посылки, проектирование БЭАО одна из самых ответственных задач в проекте ПТК «ПХВ-1».

Документация

Для ПТК «ПХВ-1» разрабатывается и предоставляется пользователю следующая документация:

Общесистемная документация:

- общее описание ПТК (ПД);
- инструкция по эксплуатации КТС (ИЭ);
- руководство по системной поддержке (ИЭ);
- описание программного обеспечения (ПА);
- ведомость машинных носителей информации.

1. На фронтальные и локальные ПЛК:

- сборочный чертёж (СБ);

- схема электрическая принципиальная (Э3);
- таблица соединений (ТЭ4);
- таблица подключения (ТЭ5);
- ведомость покупных изделий (ВП);
- ведомость ЗИП;
- паспорт (ПС);
- ведомость эксплуатационных документов (ВЭ);
- руководство по эксплуатации (РЭ);

- руководство программиста (РП);
- перечень элементов ПЭЗ.

2. На АРМ:

- Руководство пользователя (ИЗ);
- Чертежи видеокадров (ИЗ);
- Описание программного обеспечения.

Документация оформляется в соответствии с требованиями ЕСКД и ЕСПД. На составные компоненты импортного

производства пользователю предоставляется эксплуатационная документация на русском языке.

На ПТК «ПХВ-1» выпущены и действуют технические условия.

ПРИЛОЖЕНИЕ 7

Код основного модуля программы MODBUS_MASTER

```
//
*****************************
*****************************
******************
//
*******************
*************
MODBUS MASTER
*******************
************
//*****************
*******************
*******************
*******************
****
i
i
n
c
```

```
lude "comport.h"  #include <crclrc.h>  t#include "modbu
```

```
s .h"    t t i n c l u d e   < s y s / t i m e b .h >    t t i n c l u d e   < m a t h .h >
#ifdef WIN32
/*************** секция
WINDOWS
*****************/
```

```
ttdefine usleep(delay)
Sleep(delay/1000)
#endif

#include <time.h>
iinclude
<sys/timeb.h>
#include <stdio.h>

unsigned char
_mod_buffer[260];
unsigned char
_mod_ascii_buffer[MAX_
ASCII_BUF];

enum
      D
      e
      b
      u
      g
      D
      a
      t
      a
      T
      y
      p
      e
      {

      D
      A
      T
      A
      _
      D
      E
      C
      ,

      D
      A
      T
      A
      _
      H
      E
      X
      ,

      D
      A
      T
      A
```

```
_OCT,DATA BIN,DATA FLOAT,DATA
  int __mod__debugType = DATA_HEX;                  // ту
переменные
  int __mod_debugState = MOD_DEBUG_OFF;             //
управление выполнением
  int _mod_protocol_type = MODBUS_DEFAULT; //
программы

  //struct timeb
  _mod_ResponseTime;
  // время записи в
устройство и время
ответа операции
MODBUS
  long
  _mod_responseTime;                                //
время ответа в
миллисекундах
  //float _mod_charPS
  = 0; // 1/((_baud
  rate ) / ( длина в
  битах )) //------------------------------------------------------------
  // function
  pointers -
используются когда
```

```
установлен режим
DEBUG или ASCII int
(*_mod_procSendData
ToDevice)(unsigned
char devNum,
unsigned char
command, unsigned
int count) =
_mod_SendDataToDevi
ceRTU;
int
(*_mod_procGetDataF
romDevice)(unsigned
char devNum,
unsigned char
**data, unsigned
long *count) =
_mod_GetDataFromDev
iceRTU;
int
(*_mod_procRecieveD
ata)(unsigned short
*crcRet, int
*exErrorCode) =
_mod_RecieveData;
int
(*_mod_procTransmitDat
a)(int count) =
_mod_TransmitData;
/*int
(*_mod_procRecieveD
ataASCII)(unsigned
short *crcRet, int
*exErrorCode) =
_mod_RecieveDataASC
II;
int
(*_mod_procTransmit
DataASCII)(int
count) =
_mod_TransmitDataAS
CII;*/ //--------------------------------------
```

// Сканирование сети MODBUS

```
int
ScanModBus(LPMODBUS
DEVICE device) {
      r
      e
      g
      i
      s
      t
      e
```

```
r int i=MAX_DEVICE_COUNT,j=0; unsigned char *dataPt
```

```
r
;
unsigned long
nCount;
int dbgType =
GetModBusDebugTy
pe();
int dbgState =
GetModBusDebugSt
ate();
// --- Запрет
операции отладки
функции IO до
начала
сканирования ----------
// if
(dbgS
tate
==
MOD_D
EBUG_
ON) /
/
ModBu
sDebu
gEnab
le(0,
0);
printf("%d\n",
dbgState) ;
while(-i){//
Сканирование
всей сети MODBUS
функцией 0x11
i
f
(
S
e
n
d
D
a
t
a
T
o
D
e
v
i
```

```
moreDataFrom getData() if continue; if successful = -1 ) {
```

```
Developer, standaarden, tenacity == succesvol! deal
```

```
j
l
.
d
e
v
A
d
d
r
=
i
;
d
e
v
i
c
e
[
j
l
.
d
e
v
I
D
=
*
(
d
a
t
a
P
t
r
+
3
)
;
}
usleep(500
00);
}
```

```
      // -------
      Выполнение
      операции
      отладки, если
      она разрешена ----------------------------
// if
(dbgS
tate
==
MOD_D
EBUG_
ON) /
/

ModBu
sDebu
gEnab
le(1,
dbgTy
pe);
      return j;
}
```

// Получить идентификатор устройства

```
int
GetDe
vicel
D(uns
igned
char
devNu
m,
LPMOD
BUSDE
VICE
devic
e) {
      register int
      res;
      unsigned char
      *dataPtr;
      unsigned long
      nCount;
      int dbgType =
      GetModBusDebugTy
      pe();
      int dbgState =
      GetModBusDebugSt
      ate();
      // - - Запрет
операции отладки
функции IO до
начала
сканирования ----------------------------
```

```
// if (dbgState == MOD_DEBUG_ON) //
ModBusDebugEnable(0, 0);
    // Посылаем функцию 0x11 для получения информации об устройстве
    SendDataToDevice(devNum,0x11,0);
    if ((res = GetDataFromDevice(devNum,SdataPtr,SnCount)) == SUCCESSFUL){ // Полученные данные записываем в структуру
        device->devAddr = devNum;
        device->devID = *(dataPtr + 3);
    }
    usleep(50000);
    // -------
    Выполнение операции
```

```
      отладки, если
      она разрешена ----------------------------
// if
(dbgS
tate
==
MOD_D
EBUG_
ON) /
/           ModBusDebugEnable(1,
dbgTy
pe);
      return res;
}
```

// Проверка на наличие устройства с номером devNum в списке найденных устройств

```
int
IsDeviceInList(unsi
gned char
devNum,LPMODBUSDEVI
CE device,int
devCount) (
      register int
      i = devCount,
      j=0; while(i
      —){
            if
            (devNum==d
            evice[j].d
            evAddr)
            return 0;

      }
      return -1;
}
```

// Чтение дискретных выходов устройства

```
int
ReadDiscreteOut(uns
igned char devNum,
unsigned long
startAddr, unsigned
long count,
      unsigned char
      **data, unsigned
      long *nBytes)

{
      register int
      res; unsigned
      char *dataPtr;
```

```
unsigned long
nCount;
unsigned short
*ptr = (unsigned
short
*)GetDataPtr();
*ptr = EndianSwap
(startAddr) ;
Переставим старшие и
младшие байты
*(ptr+1) =
EndianSwap
(count) ;
счетчика
// Пошлем данные
устройству
if ((res =
SendDataToDevic
e(devNum,0x01,4
))!=SUCCESSFUL)
return res; //
Считаем данные из
устройства
if ((res =
GetDataFromDevic
e(devNum,
SdataPtr,
SnCount)) !
=SUCCESSFUL)
return
res;
*data = dataPtr+3;                    // data
- Содержит битовый
ряд с положением
дискретных
выходов каналов
*nBytes = *
(dataPtr+2) ; // -
Количество
значащих бит в
полученном массиве
return res;
}

// Не удалось проверить, т.к.
функция не работает в ПКЦ12
int
Rea
dDi
agn
ost
ic(
uns
```

```
ign
ed
cha
r
dev
Num
,un
sig
ned
sho
rt
*va
lue
) {
      register int
      res;
      unsigned char
      *dataPtr =
      GetDataPtr();
      unsigned long
      nCount;
      *dataPtr =
      0x00;
      *(dataPtr+1) =
      0x02;
      *(dataPtr+2) =
      0x00;
      *(dataPtr+3) =
      0x00; // *ptr =
      0x0002; //
      *(ptr+1) =
      0x0000;
      if ((res =
      SendDataToDevic
      e(devNum,0x08,4
      ))!=SUCCESSFUL)
      return res; if
      ((res =
      GetDataFromDevi
      ce(devNum,Sdata
      Ptr,&nCount))!
      =SUCCESSFUL)
      return
res;
      *value =
      EndianSwap(*((u
      nsigned short
      *)
      (dataPtr+4)));
      return res;
}

// Не удалось проверить, т.к.
функция не работает в ПКЦ12
int
Cle
```

```
arDiagnostic(unsigned char devNum) {
      register int res;
      unsigned char *dataPtr = GetDataPtr();
      unsigned long nCount;
      *dataPtr = 0x00;
      *(dataPtr+1) = 0x01;
      *(dataPtr+2) = OxFF;
      *(dataPtr+3) = 0x00; // *ptr = 0x0002; //
      *(ptr+1) = 0x0000;
      if ((res = SendDataToDevice(devNum,0x08,4))!=SUCCESSFUL) return res; if ((res = GetDataFromDevice(devNum,SdataPtr,SnCount))!=SUCCESSFUL) return
res;
      return res;
}
```

// Чтение группы регистров устройства / / Параметры:
// devNum - **номер устройства на шине MODBUS** // startAddr - **начальный адрес регистра устройства** // count - **количество регистров подлежащих прочтению** // data -

возвращается указатель
на прочитанные данные
// nRegs - **количество**
прочитанных регистров

```
int
ReadRegisters(unsigned char devNum,
unsigned long startAddr, unsigned long count,
        unsigned short **data, unsigned long *nRegs)
{
    register int status;
    register unsigned char hardware;
    register unsigned short *data;
```

```
r: unsigned long nCount: unsigned short *ptr = (unsign
```

```
ed shoot *jGeetDataPetry); *ptr = EnddianssWapplsteetAddr)
```

```
;
    *(
     ptr+1
     )
        =
         End
         ndian
         Swap
         (
         count
         )
         ;
         if ((res =
         SendDataToDevi
         ce(devNum,0x03
         ,4))!
         =SUCCESSFUL)
         return res; if
          ((res =
          GetDataFromDev
          ice(devNum,Sda
          taPtr,SnCount)
          )!=SUCCESSFUL)
          return
          res ;
           ptr =
           (unsigned
           short *)
           (dataPtr+3);
           *data = ptr;
           *nRegs =
          (*(dataPtr+2)) »
          1; /* i=*nRegs; do{
```

```
* ptr = End;ans swap(* ptr); ptr++; } while(--i);*/ return
```

```
        r
        e
        s
        ;
}
```

// Чтение группы 32-х разрядных регистров устройства / / Параметры:

// devNum - **номер устр**

на шине MODBUS

// startAddr - **начальны**

регистра устройства

// count - **количество ре**

подлежащих прочтению

// data - **возвращается у**

на прочитанные данные

// nRegs - **количест**

прочитанных регистров

```
int

ReadRegisters32(unsign
ed char devNum,
unsigned long
startAddr, unsigned
long count,
      unsigned long
**data, unsigned long
*nRegs)
{
      register int
      res; unsigned
      char *dataPtr;
      unsigned long
      nCount;
      unsigned short
      *ptr =
      (unsigned
      short
      *)GetDataPtr()
      ; *ptr =
      EndianSwap(sta
      rtAddr);
      *(ptr+1) =
      EndianSwap
      (count«1 ) ;
      if ((res =
SendDataToDevi
ce(devNum,0x03
,4))!
=SUCCESSFUL)
```

```
    return res; if
      ((res =
      GetDataFromDev
      ice(devNum,Sda
      taPtr,SnCount)
      )!=SUCCESSFUL)
      return
    res;
        ptr =
      (unsigned short *)
      (dataPtr+3); *data =
      (unsigned long
      *)ptr; *nRegs =
      (*(dataPtr+2)) >> 2;
      /* i=*nRegs; do {
                *
                  p
                  t
                  r
                  =
                  E
                  n
                  d
                  i
                  a
                  n
                  S
                  w
                  a
                  p
                  (
                  *
                  p
                  t
                  r
                  )
                  ;
                  * (
                  p
                  t
                  r
                  + 1
                  )
                  =
                  E
                  n
```

```
d
i
a
n
S
w
a
p
(
*
(
p
t
r
+
1
)
)
;
        p
        t
        r
        +
        =
        2
        ;
    }while(--i);*/
    return res;
}

// Чтение одного 32-х
разрядного регистра
устройства //
Параметры:
//
на шине MODBUS
//
регистра устройства
//
устройства значение
int

ReadRegister32(unsigne
d char devNum,
unsigned long
startAddr, unsigned
long *value) {
    register
    int res;
    unsigned
    char
    *dataPtr
```

devNum - номер устро

startAddr - начальный

value - считанное

```
;
unsigned
long
nCount;
unsigned
short
*ptr =
(unsigne
d short
*)GetDat
aPtr();
*ptr =
      EndianSw
      ap(start
      Addr);
      *(ptr+1)
      =
      0x0200;
      if ((res =
      SendDataToDevic
      e(devNum,0x03,4
      ))!=SUCCESSFUL)
      return res; if
      ((res =
      GetDataFromDevi
      ce(devNum,Sdata
      Ptr,SnCount))!
      =SUCCESSFUL)
      return
res;
      ptr = (unsigned
      short *)
      (dataPtr+3); if
      (*(dataPtr+2)!
      =4) return
      READ_ERROR;
      *ptr =
      EndianSwap(*ptr
      ); *(ptr+1) =
      EndianSwap(*(pt
      r+1)); *value =
      *((unsigned
      long*)ptr);
      return res;
}
```

// Чтение одного 16-ти разрядного регистра устройства / /
Параметры:
// devNum - **номер устр**
на шине MODBUS

```
//                                    startAddr - начальный
регистра устройства
//                                    value - считанное
устройства значение
int

ReadRegister16(unsigne
d char devNum,
unsigned long
startAddr, unsigned
short *value) {
      register int
      res; unsigned
      char *dataPtr;
      unsigned long
      nCount;
      unsigned short
      *ptr =
      (unsigned short
      *)GetDataPtr();
      *ptr =
      EndianSwap(star
      tAddr);
      *(ptr+1) =
      0x0100;
      if ((res =
      SendDataToDevic
      e(devNum,0x03,4
      ))!=SUCCESSFUL)
      return res; if
      ((res =
      GetDataFromDevi
      ce(devNum,Sdata
      Ptr,SnCount))!
      =SUCCESSFUL)
      return
res;
      ptr = (unsigned
      short *)
      (dataPtr+3); if
      (*(dataPtr+2)!
      =2) return
      READ_ERROR;
      *value =
      EndianSwap(*ptr
      ); return res;
}
```

//При записи используются все те же параметры что и при чтении

```
int
WriteRegisters(u
nsigned char
```

```
devNum, unsigned
long startAddr,
unsigned long
count,
      unsigned short
      *data,unsigned
      long *regStart,
      unsigned long
      *nRegs)
{
      register int
      res;
      unsigned char
      *dataPtr =
      GetDataPtr();
      unsigned long
      nCount;
      unsigned char
      byteCount;
      unsigned short
*ptr = (unsigned short
*)dataPtr;
      *ptr =
EndianSwap(startAddr);
      *(ptr+l) =
EndianSwap(count);
      byteCount =
(count&OxFF) <d;
      *(dataPtr+4) =
byteCount;
      ptr = (unsigned
short *) (dataPtr+5);
      memcpy (ptr,
data, counted) ;
      if ((res =
SendDataToDevice(dev
Num,0x10,5 +
byteCount))!
=SUCCESSFUL) return
res;
      if ((res =
GetDataFromDevice(devN
um,SdataPtr,SnCount))!
=SUCCESSFUL) return
res;
      ptr =
      (unsigned
      short *)
      (dataPtr+2);
      *regStart =
EndianSwap(*pt
r); "nRegs =
EndianSwap(*(p
```

```
      tr+1)); return
      res;
}
int
WriteRegister16(unsign
ed     char     devNum,
unsigned          long
startAddr, unsigned
short value) {
      register int       res;
      unsigned char
      *dataPtr =
      GetDataPtr();
      unsigned long
      nCount;
      unsigned char
      byteCount;
      unsigned short
*ptr = (unsigned short
*)dataPtr;
      *ptr =
EndianSwap(startAddr);
      *(ptr+1) =
0x0200;
      byteCount = 2;
      *(dataPtr+4) =
byteCount;
      ptr = (unsigned
short *)(dataPtr+5);
      *ptr =
EndianSwap(value);
      if ((res =
SendDataToDevice(dev
Num,0x10,5 +
byteCount))!
=SUCCESSFUL) return
res;
      if ((res =
GetDataFromDevice(devN
um, SdataPtr,
SnCount)) !
=SUCCESSFUL) return
res;
      return res;
}

int
WriteRegisters32(uns
igned char devNum,
unsigned long
startAddr, unsigned
long count,
      unsigned long
*data,unsigned long
```

```
*regStart, unsigned
long *nRegs)
{
      register int
res;
      unsigned char
      *dataPtr =
      GetDataPtr();
      unsigned long
      nCount;
      unsigned char
      byteCount;
      unsigned short
*ptr = (unsigned short
*)dataPtr;
      *ptr =
EndianSwap(startAddr);
      * (ptr+1) =
EndianSwap (counted) ;
      byteCount =
((count<<l) sOxFF) «1;
      *(dataPtr+4) =
byteCount;
      ptr = (unsigned
short *)(dataPtr+5);
      memcpy(ptr,data,
count<<2) ;
      if ((res =
SendDataToDevice(dev
Num,0x10,5 +
byteCount))!
=SUCCESSFUL) return
res;
      if ((res =
GetDataFromDevice(devN
um,
SdataPtr,SnCount))!
=SUCCESSFUL) return
res;
      ptr = (unsigned
      short *)
      (dataPtr+2);
      *regStart =
      EndianSwap(*ptr)
      ; *nRegs =
      EndianSwap(*(ptr
      +1)); return
      res;
}
int
WriteRegister32(unsign
ed char devNum,
unsigned long
startAddr, unsigned
```

```
long value) {
      register int      res;
      unsigned char
      *dataPtr =
      GetDataPtr();
      unsigned long
      nCount; unsigned
      char byteCount;
      unsigned short
            *ptr =
            (unsigned
            short
            *)dataPtr;
      *ptr =
            EndianSwap
            (startAddr
            );
      *(ptr+1) =
            0x0200;
      byteCount = 4;
      *(dataPtr+4) =
            byteCount;
      ptr = (unsigned
            short *)
            (dataPtr+5
            );
      *ptr =
      EndianSwap((unsi
      gned short)
      (value &
      OxFFFF));
      *(ptr+1) =
      EndianSwap((unsi
      gned short)
      (value>>16));
      if ((res =
SendDataToDevice(devNu
m,0x10,5 +
byteCount))!
=SUCCESSFUL) return
res;
      if ((res =
            GetDataFro
            mDevice(de
            vNum,Sdata
            Ptr,&nCoun
            t))!
            =SUCCESSFU
            L) ret
res;
      return res;
}
```

```
//**********
Возвращает ответ
устройства в
миллисекундах
******************** /
/*********************
**********************
**********************
**********
long GetResponseTime()
{ return
_mod_responseTime;}

/
y*********************
**********************
***********
jy****************
Вывод сообщения об
ошибке
**********************
**********
//*********************
**********************
**********************
***********
void
_mod_PrintError(int
err) {
      printf("***
      MODBUS ERROR %d
      ***: ",err);
      switch(err){
            case
            ILLEGAL_FU
            NCTION   :
      printf(MSG_ILLEG
            AL_FUNCTIO
            N);break;
            case
            ILLEGAL_DA
            TA_ADDRESS
            :
      printf(MSG_ILLEG
            AL_DATA_AD
            DRESS);bre
            ak;
            case
            ILLEGAL_DA
            TA_VALUE  :
      printf(MSG_ILLEG
            AL_DATA_VA
            LUE);break
            ;
            case
            SLAVE_DEVI
            CE_FAILURE
            :
```

```
printf(MSG_SLAVE
       _DEVICE_FA
       ILURE);bre
       ak;
       case
       ACKNOWLEDG
       E      :
         printf(MSG
         _ACKNOWLED
         GE);break;
         case
         SLAVE_DEVI
         CE_BUSY   :
       printf(MSG_SLAVE
         _DEVICE_BU
         SY);break;
         case
         NEGATIVE_A
         CKNOWLEDGE
         :
       printf(MSG_NEGAT
         IVE_ACKNOW
         LEDGE) ;br
         eak;
         case
         MEMORY_PAR
         ITY_ERROR :
       printf(MSG_MEMOR
         Y_PARITY_E
         RROR);brea
         k;
         default:
                p
                r
                i
                n
                t
                f
                (
                "
                u
                n
                d
                e
                f
                i
                n
                e
                d
                   e
                   r
```

```
                r
                o
                r
                "
                )
                ;
                b
                r
                e
                a
                k
                ;
        }
```

ПРИЛОЖЕНИЕ S

Экранный снимок программы MUDBUS MASTI-K

```
icrosoft Windows
XP [Версия
5.1.2600 CO
Корпорация
Майкрософт,
1985-2001.
C:\Docui4ents and
SettingsSAnMHMHCTpaTop>c
d..
C:\DocUMonts and
Settings)cd..
C: \ )no dbus пав t e
r. e xe
modbusmaster uZ.l
usage : mo dbus
piaster
[options] [long
options] long
options:
COM port options:
     con
     [port],[baudrate],
     [format 3,[flow]
     [port]
     port nane
     </dev/ttyS0)
     [baudrate] —
     set con port
     baudrate
```

```
  - data
format In
special form:
[XHPHS], i.e.
8N1
      where [X]
— number
bits of
data
[5..81 <8
— by
default>
      [PI
      -
      pari
      ty
      type
      :
      (N<n
      one)
      ,
      0(od
      d>,
      E<ev
      en)3
      <N -
      by
      defa
      ult?
      [S3
      -
      numb
      er
      of
      stop
      bits
      [1,2
```

```
                                                                  3 <1
                                                                  - by
                                                                  defa
                                                                  ult>
                                                  — flow control:
                                                  [none, soft,
                                                  hard, both3
                                                  (none — by
                                                  default)
                                        [flow]
MODBUS options: —node
```


- register
index that must
be read or
write
ng that would
transmit to
register<s) or
to device
- set byte
numltar in
message which
point to a
number
items to read
-scan - perform
a full MODBUS net scan
for any devices -
listen - listen COM
port short options:
rt debug mode,
data type
visualization:
dec,bin,hex.oct
,float] <by
default - hex)
-c ~ automatic
calculation CRC
of the BflU
data
ister of the
device
according the
following
format: b -
print data as
BIN
- p r i n t d a t a a s O

```
CTh - print data as HEX
```

```
 — print data as float c —
 print data as set of chars
 print data as DEC by default
 -w - write register<s) or raw data:

 2 ~ write data to 32 bit register 16 - write data to 16 bit register raw - write raw data to port <with/without) CRC -e — endiari type:

 - use in register operation big endians

 use in register operation little endians

 f both parameters are set ~ use half big endians (only 2 numbers)

  enable ASCII mode Cnot fully supported )

  print device response tine

  listen COM port
```

verbose

ПРИЛОЖЕНИЕ 9

АКТЫ ВНЕДРЕНИЯ

«Утверждаю»
Генеральный директор
ООО «ПСВ-Холдинг»

/
/
7

Д. Ю. Пунин

АКТ ВНЕДРЕНИЯ

Результаты исследований, полученные Дерябиным А.В. при выполнении диссертационной работы, в частности:

Методики и рекомендации по обеспечению информационной безопасности каналов связи в АСУТП, а также рекомендации по выбору программных и аппаратных средств для проектирования автоматизированной системы управления технологическими процессами, соответствующих стандартам и требованиям по безопасности в химической промышленности.

внедрены в 2008-2009 году на нашем новом производственном предприятии в г.Электросталь, Московской области - в АСУТП комплекса по производству поливииилхлорида и бумвинила.

Методики и рекомендации позволили существенно облегчить работу проектировщиков при выборе методов и средств защиты информации. Методики позволили повысить защищенность информации и телекоммуникаций в АСУТП предприятия. Выработанные методики позволили снизить количество сбоев в технологическом процессе из-за искажения или потери информации, что положительно сказалось на качестве выпускаемой продукции.

С
Лохиов М. В.

Семенов А. А.

Главный инженер к.т.н.

Главный технолог:

Генеральный директор
ООО «ТЕЗА-Сервис»

А. В. Маров

АКТ
ВНЕ
ДРЕ
НИЯ

Результаты, полученные Дерябиным А.В. при выполнении диссертационной работы, в частности:

- Методики защиты телекоммуникаций АСУТП верхнего и нижнего уровней;
- Рекомендации по обеспечению защиты проводных и беспроводных каналов связи АСУТП и SCADA-систем;

внедрены на объектах проектируемых и обслуживаемых нашим предприятием в 2008 году и будут внедряться в дальнейшем.

Методики показали высокую эффективность и позволили существенным образом увеличить защищенность передаваемой информации и всей системы в целом
.

Главный инженер: к. т, Сергеев М. А.

Руководитель проектной группы: Кирилленко С. В.

Акт внедрения

Результаты, полученные **Дерябиным А**.В. при выполнении диссертационной работы, в частности:

1) Методики применения различных способов защиты информации от несанкционированного доступа в АСУТП;

2) Рекомендации по защите телекоммуникационных и компьютерных сетей;

внедрены на нашем предприятии в 2008-2009гг. Они нашли практическое применение при обмене информацией с нашими филиалами в гг. Иваново, Санкт-Петербург, Омске и т.п.

Указанные методики хороши тем, что при сравнительно небольших затратах обеспечивают высокую эффективность и не требуют специальной подготовки нашего персонала.

«Утверждаю»
Генеральный директор
НПО «РИК»,
А. В. Поляков

Сирко С. Э.

Начальник отдела-

Начальник лаборатории

Смушко О.Л.

*(m) /**
192