МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Российский технологический университет»

МИРЭА

Институт информационных технологий

наименование института (полностью)

Кафедра промышленной информатики

наименование кафедры (полностью)

УТВЕРЖДАЮ

и.о. Зав. кафедрой ПИ

_____/В.А. Макаров/

«___»_____20__

КОНСПЕКТ ЛЕКЦИЙ ПО ДИСЦИПЛИНЕ

Защита информации в информационно-управляющих системах

(наименование дисциплины)

Направление подготовки **09.04.01 Информатика и вычислительная техника**

(код и наименование)

Форма обучения **очная**

(очная, очно-заочная, заочная)

Магистерская программа **Информационно-управляющие системы**

(академический, прикладной бакалавриат)

Квалификация выпускника **Магистр**

Москва 2018

Оглавление

1. ОБЩАЯ ХАРАКТЕРИСТИКА АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

Текст взят из книги Т.А. Пьявченко, В.И. Финаев. Автоматизированные информационно-управляющие системы. - Таганрог: Изд-во ТРТУ, 2017. - 271 с.

Системой управления называется система, в которой реализуется процесс управления путем взаимодействия объекта управления и управляющей части. Различают автоматические и автоматизированные (информационно-управляющие) системы управления. В системах автоматического управления (САУ), состоящих из объекта управления и управляющего устройства (управляющей части), человек непосредственного участия в процессе управления не принимает. В автоматизированных системах управления (АСУ) предполагается обязательное участие людей в процессах управления. Сбор, анализ и преобразование информации в информационно-управляющих системах выполняется с помощью вычислительной техники.

Эффективное решение задач управления в настоящее время немыслимо без привлечения средств вычислительной техники и всевозможных автоматизированных информационно-управляющих систем (ИУС), в число которых входят автоматизированные системы управления технологическими процессами (АСУТП). ИУС и АСУТП создаются для совершенствования управления отраслями и отдельными предприятиями на основе применения математических методов, современных средств вычислительной техники и средств связи для наилучшего использования производственных фондов, увеличения выпуска продукции, снижения ее себестоимости, повышения производительности труда, рентабельности производства и роста прибылей.

1.1. Системный анализ задач управления

Рост числа производственных и информационных связей между отдельными предприятиями и учреждениями, повышение эффективности производства, перепрофилирование предприятий в условиях рынка сопровождаются ростом сложности процессов управления и систем управления. Увеличение объема информации, охватывающей все стороны производства, с ростом самого производства приводит к значительному усложнению задач управления.

На рис. 1.1 представлена укрупненная схема предприятия, включающая производство, организацию и управление. Производственное предприятие, упрощенно показанное в виде прямоугольника, состоит из трех блоков:

A - подготовка и обслуживание производства;

B - собственно производство;

C - сбыт готовой продукции.

Рисунок 1.1 - Укрупненная схема предприятия.

В блок А входят склады сырья и исходных материалов, ремонтные, транспортные цехи, службы информации, связи и др. Блок В состоит из цехов основного производства, включающих технологические агрегаты, конвейерные и транспортные линии, склады полуфабрикатов и др. Блок С – сбыт готовой продукции подразумевает, в основном, склады готовой продукции. Основу производства составляют оборудование, производственный персонал, материальные, энергетические, информационные и др. ресурсы. Управление предприятием показано в виде треугольника, состоящего из трех «слоев». Внутри и снаружи треугольника управления циркулируют информационные потоки. Сверху вниз - управляющие воздействия, снизу вверх - информация обратной связи, по горизонтали - обмен информацией между внутренними объектами одного уровня, а также между внутренними и внешними объектами. Механизм управления включает в себя управленческий персонал, компьютерные сети, финансовые, информационные и другие ресурсы. Задача управления производством сводится к рациональному управлению потоками ресурсов: материальных, энергетических, финансовых, информационных и др. Основание треугольника — это системы сбора, обработки, хранения, передачи и представления информации – информационная система (ИС). ИС представляют собой информационную модель предприятия, которая отображает не только текущее состояние предприятия, но и состояние за прошедшие периоды времени. Во многих случаях требуется хранить информацию о готовой продукции, исходных и промежуточных материалах, технологических режимах, состоянии оборудования, сведения об исполнителях и др. в течение нескольких лет. На вершине треугольника управления находятся руководители предприятия, принимающие решения и образующие системы принятия решений (СПР). Каждое предприятие стремится достичь определенных целей своей деятельности. Целей деятельности бывает несколько. У разных предприятий они могут

существенно отличаться, но две из них одинаковы для всех предприятий. Первая цель - социальная, направленная на пользу общества (например, производство необходимой обществу продукции, обеспечение необходимым количеством рабочих мест, защита окружающей среды и др.), а вторая цель - экономическая, заключающаяся в получении от деятельности предприятия максимальной прибыли. В системном анализе существует задача структуризации целей.

Между основанием треугольника управления и его вершиной находится среднее звено специалистов, образующее системы поддержки принятия решений (СППР). Эти специалисты выполняют многовариантные расчеты, используя полученные от р54уководителей значения критериев оптимальности и значения ограничений, а также полученные от объектов фактические значения контролируемых параметров производства». Из сказанного выше можно сделать вывод: большинство интегрированных систем управления производством имеют иерархическую структуру, объединяющую функции АСУП – автоматизированных систем управления производством и АСУТП – автоматизированных систем управления технологическими процессами (см. рис. 1.2).

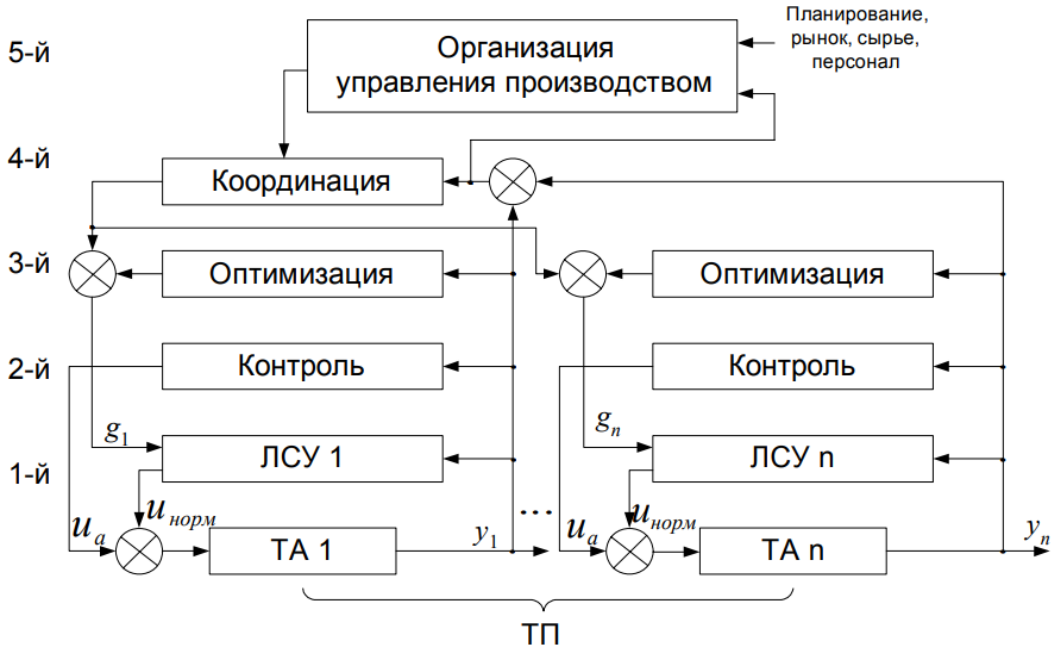

Рисунок 1.2 - Иерархическая структура управления производством

Как видно из рис. 1.2, на нижнем уровне с помощью локальных систем (ЛСУ) осуществляется непосредственное управление технологическим объектом – технологическим агрегатом (ТА) по измеряемым координатам y. Для реализации закона управления используются либо промышленные регуляторы, либо контроллеры. При этом сигнал задающей переменной g формируется на более высоком уровне в зависимости от принятого критерия управления. В частности, он может быть постоянным при задании от уровня координации, на котором происходит распределение нагрузки на технологические агрегаты, либо изменяться в зависимости от величины функционала оптимизации на 3-м уровне управления. Уровни управления 5-й, 4-й и 3-й можно отнести к функциям АСУП, поскольку современное производство не может быть эффективным без учета потребностей рынков сбыта, качества и объема сырья, а также квалификации обслуживающего персонала. К функциям АСУТП, помимо ЛСУ, следует отнести функции контроля (2-й уровень), предназначенные для выявления предаварийных

ситуации по отклонению технологических параметров от допустимых значений. В случае обнаружения недопустимых отклонений система вырабатывает управление по аварии ua (например, отключение питания или прекращение подачи топлива и т.п.), одновременно отображая на мнемосхеме ТП и фиксируя в отчете тревог информацию о причине аварии. Тенденция развития современных систем управления сложными процессами заключается в создании адаптивных интеллектуальных систем, функционирование которых невозможно без использования развитой вычислительной сети, включающей персональные компьютеры (ПК), микроконтроллеры и широкий набор модулей ввода/вывода.

Решение различных задач управления должно производиться на основе единого системного подхода как при проектировании автоматизированных информационно-управляющих систем, так и при эксплуатации этих систем.

Сущность системного подхода состоит во взаимосвязанном, комплексном изучении сложных объектов как целостных систем с определенными системными целями и согласовании целей системы и ее частей и подсистем в процессе функционирования.

Комплексность означает одновременное рассмотрение разных задач управления, а системность означает рассмотрение всех их во взаимосвязи, упорядоченно по месту, времени, ресурсам, в рамках единого целого, выделенного из окружающей среды.

Использование системного подхода при проектировании ИУС состоит в выделении и представлении некоторой совокупности объектов и связей между ними в виде системы, в правильном понимании происходящих в них явлений, взаимодействий, умении выделить и поставить первоочередную (главную) группу задач.

Практически все явления в природе и обществе априори неопределены, имеют стохастический характер, поэтому подход при исследовании их должен быть не только системным, а системно-вероятностным. Применение

вероятностного подхода позволяет формализовать существующую неопределенность в Борелевском пространстве с применением вероятностной меры. Однако вероятность является объективным понятием, а на практике для оценки вероятности события применяют обработанные статистические данные. Появляется задача значимости и достоверности оценки вероятности, зависящая от репрезентативности выборки.

На наш взгляд более эффективным подходом является применение методов искусственного интеллекта, эвристических алгоритмов для решения задач управления сложными объектами. При применении данного подхода параметры, характеризующие объект и определяющие исходные данные для принятия решений, задаются в виде лингвистических переменных. Необходимость применения лингвистических переменных в подобных ситуациях определяется следующим образом. Знание специалистов можно формально определить экспертным путем. Для этого необходимо определить некоторое базовое множество возможных цифровых оценок X, смысловое название входного фактора.

Определение системы. Понятие системы в настоящее время стало в кибернетике и системотехнике исходным и доминирующим, и позволяет выделить из окружающей реальности по ряду признаков обособленный объект (группу объектов) и рассматривать этот объект как совокупность взаимосвязанных частей - элементов и вместе с тем как элемент более общей системы - среды.

Понятия строения и функционирование систем. Понятия определяются одно через другое, уточняя друг друга. Под элементом понимается простейшая, неделимая часть системы. Понятие неделимости является неоднозначным. Поэтому элемент - это предел членения системы с точки зрения аспекта рассмотрения решения конкретной задачи, поставленной цели. Сложные системы вначале делят на подсистемы или на компоненты. Подсистема - это относительно независимая часть системы, обладающая ее

свойствами, имеющая подцель, на достижение которой ориентирована подсистема. Если части системы не обладают всеми ее свойствами, а представляют собой совокупности однородных элементов, то такие части принято называть компонентами. Связь характеризует и строение (статику) и функционирование (динамику) системы. Известны три типа связей между элементами: функционально необходимые, сингерические (которые при кооперативных действиях некоторых частей обеспечивают увеличение их общего эффекта до величины, большей суммы эффектов от тех же независимо действующих частей), избыточные (являются излишними или противоречивыми). Связь определяют как ограничение степени свободы элементов. Элементы, вступая во взаимодействия друг с другом, утрачивают часть своих свойств, которыми они потенциально обладали. Связи характеризуются направлением, силой, характером (или видом).

Связи бывают направленные и ненаправленные, сильные и слабые. По характеру различают связи подчинения, связи порождения (или генетические), равноправные (или безразличные), связи управления. Важную роль играет обратная связь. Она может быть положительной, т.е. сохраняющей тенденции происходящих в системе изменений того или иного выходного параметра, и отрицательной - противодействующей изменениям выходного параметра, стабилизирующей его требуемое значение. Обратная связь является основой саморегулирования, развития систем, приспособления их к изменяющимся условиям существования. Понятие цель и связанные с ним понятия целесообразности, целенаправленности лежат в основе развития системы. В понятие цель вкладывают разные оттенки - от идеальных устремлений до конечных результатов, достижимых в пределах некоторого интервала времени. Под структурой системы понимают относительно устойчивый порядок внутренних пространственных связей между ее отдельными элементами, определяющий функциональное назначение системы и ее взаимодействие с внешней средой. Структура отражает определенные

взаимосвязи, взаиморасположение составных частей системы, ее устройство (строение).

В сложных системах структура включает не все элементы и связи между ними, а лишь наиболее существенные компоненты и связи, которые мало меняются при текущем функционировании и обеспечивают существование системы и ее основных свойств. Одна и та же система может быть представлена разными структурами в зависимости от стадии познания. Существуют понятия, характеризующие функционирование и развитие систем. Понятие состояние характеризует мгновенную фотографию системы, «остановку» в ее развитии. Состояние определяют через входные воздействия и выходные сигналы, либо через макропараметры, макросвойства системы. Если система способна переходить из одного состояния в другое, то говорят, что она обладает поведением. Этим понятием пользуются, когда неизвестны закономерности перехода из одного состояния в другое. Говорят, что система обладает каким-то поведением, и выясняют его характер, алгоритм. Под целостностью (эмерджетностью) системы понимается принципиальная несводимость свойств системы к сумме свойств составляющих ее элементов и невыводимость из последних свойств целого (т.е. системы). Понятие равновесия определяют как способность системы в отсутствии внешних возмущений (или при постоянных воздействиях) сохранять свое состояние сколь угодно долго. Это состояние называется состояние равновесия. Под устойчивостью понимают способность системы возвращаться в состояние равновесия после того, как она была из этого состояния выведена под влиянием внешних возмущающих воздействий или внутренних воздействий, если в системе есть активные элементы. Состояние равновесия, в которое система способна возвращаться, называют устойчивым состоянием равновесия. Понятие развитие объясняет сложные термодинамические и информационные процессы в природе и обществе. Исследование процессов развития, соотношения развития и устойчивости, изучение механизмов,

лежащих в их основе, - наиболее сложные задачи теории систем. Понятие структуры системы реализуется через элементы и связи системы. Структура - это устойчивое единство элементов и отношений в системе. Под организацией понимается, с одной стороны, свойство системы, проявляющееся в сохранении устойчивости ее структуры при различных взаимодействиях, с другой стороны, - совокупность внутренней структуры и внешних функций (поведения), присущих системе.

Изменение состояния системы влияет на состояние ее выходов. Желаемое состояние выходов называется целью системы, а функция, определяющая изменение состояния выходов, — целевой функцией системы. Для оценки отклонения фактического состояния выходов от желаемого вводится критерий цели. Исходя из двух трактовок системы можно по типу элементов их классифицировать на физические (материальные) и абстрактные (концептуальные).

1.2. Информационно-управляющие системы

Основным назначением информационно-управляющих систем (ИУС) является автоматизированный контроль и управление основными и вспомогательными технологическими процессами, противоаварийная и противопожарная защиты оборудования, контроль загазованности в помещениях и на площадках объектов разрабатываемого производства, интеграция технологических объектов в единый комплекс.

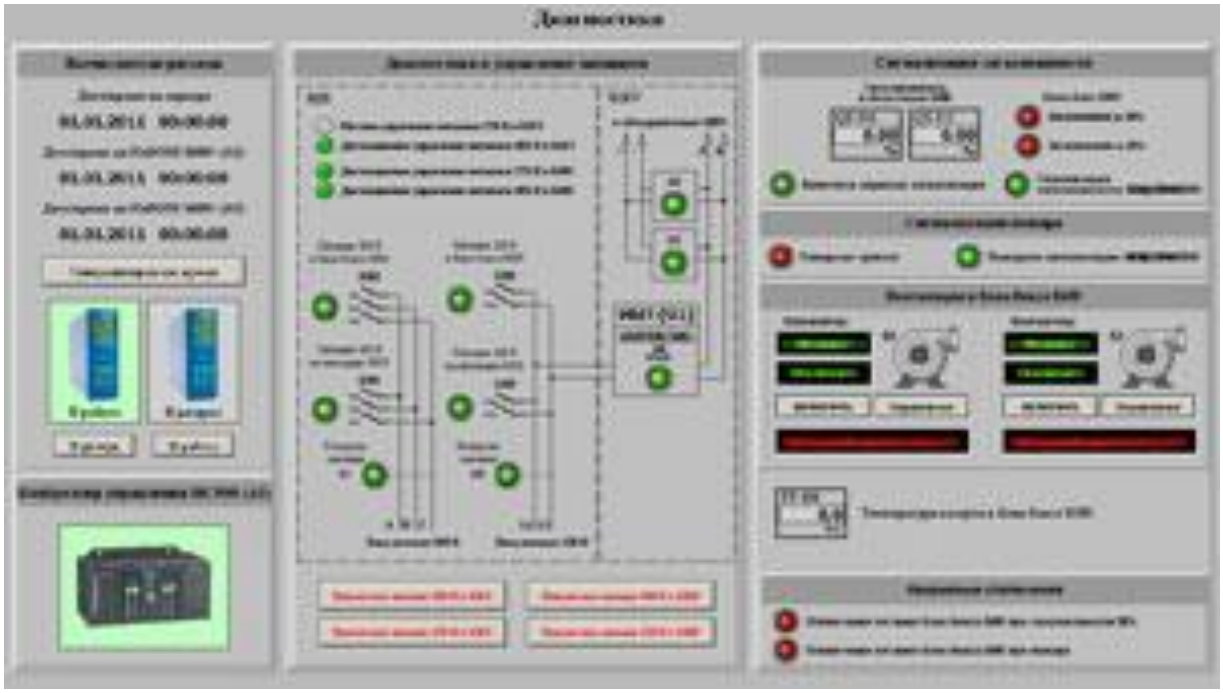

Рисунок 1.3. ИУС

Состав информационно-управляющей системы определяется техническим заданием и в общем случае содержит следующие компоненты:

- автоматизированные системы оперативно-диспетчерского управления;
- автоматизированные системы управления технологическими процессами;
- системы противоаварийной защиты;
- системы автоматического пожаротушения и контроля загазованности;
- системы телемеханики;
- автоматизированные системы управления энергообеспечением.

1.3. Особенности и классификация информационно-управляющих систем

Основоположником теоретических основ построения АСУ является академик Глушков В.М. Им была предложена классификация

автоматизированных систем. Особых изменений в этой классификации не произошло до настоящего времени, поэтому рассмотрим эту классификацию. ИУС, как автоматизированная система – это человеко-машинная система, использующая современные средства электронно-вычислительной техники, микропроцессорных систем управления и связи, экономико-математические методы, а также новые организационные принципы управления для отыскания и реализации на практике наиболее эффективного управления соответствующим объектом (системой). ИУС обладают всеми наиболее характерными чертами сложных технических систем. К ним следует отнести:

- большой масштаб систем по числу составляющих элементов и выполняемых функций;
- наличие функциональной целостности, общего назначения и цели;
- сложную многоуровневую иерархическую структуру;
- высокую степень автоматизации, определяющую известную степень самостоятельности поведения системы;
- статистически распределенные во времени внешние воздействия.

В экономических (организационных) информационно-управляющих системах в качестве элементов рассматривают: средства производства (установки, оборудования, инструмент); предметы труда (сырье, материалы, полуфабрикаты), трудовые ресурсы (рабочие, инженерно-технические работники, служащие); техническую и технологическую документацию (чертежи, инструкции, стандарты, управляющие и отчетные документы и пр.). Работы в области автоматизации процессов управления требуют глубокого анализа сущности автоматизируемых процессов, выделения объектов автоматизации, правильного формулирования целей управления и определения этапности автоматизации с учетом реальных сроков, возможностей технической реализации и экономических факторов. Объектом управления в информационно-управляющей системе может быть рабочее место, конвейер, участок, цех, предприятие, объединение и т.д. К объекту

управления относят ту часть элементов, которые непосредственно участвуют в процессе материального производства и его обслуживания. К управляющей части системы относят множества элементов, необходимых для осуществления процесса управления объектом. Это управленческий персонал, технические средства и методы управления.

Управляющая часть системы оперирует с документами. Поэтому для эффективного управления производственной системой необходим непрерывный обмен информацией между объектом управления и управляющей частью.

В управляющую часть информация поступает от вышестоящих организаций (план производстсва, директивные указания) и от объекта управления (сведения о поступлении материалов, деталей, комплектующих изделий, притоке рабочей силы; о выпуске продукции и ее качестве, затратах материалов и труда, о причинах, нарушающих протекание производственных процессов - срыве поступления материалов, поломках оборудования, браке). Управляющая часть вырабатывает управляющие воздействия на объект управления и отчетную информацию для вышестоящих организаций. Процесс выработки управляющего воздействия на объект управления имеет следующие этапы: определение цели воздействия и установление возможных изменений в других подсистемах; разработка путей, методов и средств воздействия; создание организационной системы; принятие решения, его внедрение; контроль хода внедрения; коррекция воздействия в ходе реализации принятого решения. Современные ИУС представляют собой человеко-машинные системы, в которых сочетается машинная переработка информации с координирующей деятельностью человека-оператора. За человеком остаются наиболее сложные, не поддающиеся формализации задачи, такие, например, как постановка проблемы, принятие решения в условиях неполной информации и неопределенности, контроль переработки информации. Поэтому важной задачей при создании информационно-

управляющей системы является правильное распределение функций между человеком и ЭВМ.

Функционирование информационно-управляющей системы связано и с решением ряда проблем правового, а также психологического и социологического характера. Оптимальная структура системы связана с пределами личной компетенции, формами санкций, поощрений и т. д. Эти вопросы должны решаться на правовой основе в виде должностных инструкций и предписаний, утвержденных и обязательных для исполнения. Основная цель автоматизации организационного управления - обеспечение оптимального функционирования объекта управления (предприятия, объединения, отрасли и т.п.) путем правильного выбора целей и средств их достижения с учетом имеющихся ограничений, наилучшего распределения заданий между отдельными частями, из которых состоит объект, и обеспечения их четкого взаимодействия.

По характеру производства различают АСУТП для непрерывных производств, для производств с дискретным технологическим циклом и для производств со смешанными, непрерывно-дискретными технологическими процессами. АСУТП первого типа создаются на предприятиях химической, энергетической, нефтеперерабатывающей и ряда других отраслей промышленности с непрерывными технологическими процессами.

АСУТП второго типа внедряются на предприятиях машиностроительной, приборостроительной, радиотехнической, электротехнической и других отраслей промышленности, где производство имеет дискретный характер. На таких предприятиях используется на рабочих местах универсальное оборудование, за каждым рабочим местом закрепляется множество операций; для дискретного производства присуще наличие большого количества изделий и деталей, отличающихся трудоемкостью изготовления, технологическими маршрутами, длительностью производственного цикла, а также дискретность параметров процессов.

Дискретная информация о параметрах процессов формируется вручную с помощью документов (накладных, нарядов) и различных устройств ручного ввода цифровой и алфавитно-цифровой информации, а частично от датчиков. К производствам непрерывно-дискретного типа относятся предприятия металлургической, цементной, пищевой и других отраслей промышленности.

1.4. Общая характеристика систем управления технологическим процессом

Объектом управления является технологический процесс. Под технологическим процессом как объектом управления может пониматься или последовательность целенаправленных (с использованием орудий труда) действий по получению из определенных исходных материалов конечного продукта с требуемыми свойствами, или комплекс технологического оборудования, реализующего процесс с использованием соответствующих энергоносителей и поддержанием необходимых технологических режимов. АСУТП с входящей в ее состав ИУС - это система, которая при участии операторского персонала обеспечивает в реальном времени автоматизированное управление процессом изготовления (переработки) продукта по заданным технологическим и технико-экономическим критериям. Такая система предусматривает участие в управлении процессом на подготовительных, вспомогательных, контрольных и других операциях человека. Таким образом, автоматическая система является предельным случаем автоматизированной информационно-управляющей системы.

1.5. Информационное обеспечение ИУС

Информационное обеспечение ИУС представляет собой совокупность данных, языковых средств описания данных, методов организации, хранения, накопления и доступа к информационным массивам, обеспечивающих выдачу всей информации, необходимой в процессе решения функциональных задач и

справочной информации пользователям ИУС. Данные систематизируют в специальные массивы - информационную базу ИУС. В состав информационной базы входят:

- нормативные и справочные данные, составляющие информационный базис системы;
- текущие сведения о состоянии управляемых объектов;
- текущие сведения, поступающие извне и требующие ответной реакции системы или влияющие на алгоритмы выработки решений;
- накапливаемые учетные и архивные сведения, необходимые для планирования и развития.

Поступающие в систему текущие сведения называют оперативной информацией. Средства формализованного описания данных предназначены для эффективного поиска и идентификации необходимых данных в массивах, а также для организации доступа к данным внешних абонентов ИУС. Эти средства включают в себя используемые системы классификации и кодирования объектов и информационных языков для описания запросов к информационной базе и ответов системы. Контролируют входные данные и ведение информационной базы - программные средства. В качестве таких средств обычно выступают системы управления базами данных (СУБД). Основные элементы системы информационного обеспечения ИУС - информационные массивы, предназначенные для постоянного или временного хранения информации. Необходимость в организации информационных массивов в системах информационного обеспечения АИУС:

- несовпадением моментов поступления информации с моментами ее потребления;
- необходимостью хранения исходной информации, промежуточных и окончательных результатов в процессе исполнения программ и других процедур преобразования

информации;

- использованием одних и тех же данных различными процедурами, выполняемыми как параллельно, так и последовательно;
- многократным длительным использованием некоторых данных различными процедурами.

Основные требования к информационному обеспечению:

- полнота отображения и достоверность информации;
- высокая эффективность методов и средств сбора и хранения, накопления, обновления, поиска и выдачи данных;
- одноразовый ввод информации, многократное и многоцелевое использование информации;
- простота и удобство доступа к данным информационной базы;
- ввод и накопление в информационной базе данных с минимумом дублирования;
- организация эффективной системы документооборота;
- развитие информационного обеспечения путем наращивания данных и организации новых связей и проектирования более совершенных методов и способов обработки информации;
- регламентация доступа к данным с различным уровнем доступа, а также времени хранения документированной информации.

2. ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ

Текст взят из открытого электронного ресурса https://www.securitylab.ru/analytics/486106.php. Автор Владимир Скляр

2.1. Понятие безопасности

Сегодня, пожалуй, никто особенно не задумывается, что именно вкладывается в понятие «безопасность», и так все ясно: информационная безопасность (security). Однако, есть еще и другая сторона безопасности, safety, связанная с рисками для здоровья и жизни людей, а также окружающей среды. Поскольку информационные технологии сами по себе опасности не представляют, то обычно говорят о функциональной составляющей, то есть о безопасности, связанной с правильным функционированием компьютерной системы. Если информационная безопасность стала критична с появлением интернета, то функциональная безопасность рассматривалась и до появления цифрового управления, ведь аварии происходили всегда.

Заслуживает ли внимания функциональная безопасность? Важна ли функциональная безопасность на сегодняшний день? Ведь фокус внимания в основном направлен на информационную безопасность.

С одной стороны, функциональная безопасность напрямую связана с надежностью аппаратной составляющей, и здесь осталось немного нерешенных задач, электроника безотказно работает годами, а если и этого недостаточно, то всегда есть возможность резервирования. Но ведь есть еще программная составляющая, на которую как раз и возлагается управление функциями безопасности. Существует множество примеров, когда ошибка в софте систем управления космическими системами обходилась в миллионы долларов, и это далеко не все известные случаи. А еще есть системные проекты, включающие механическую, электронную и электрическую составляющие, и здесь, к сожалению, тоже есть место для ошибок.

Одним из потенциальных рисков для интернета вещей является перехват управления на уровне физических устройств. Тогда злоумышленник может заставить систему управления выполнять опасные функции. В этом случае информационная и функциональная безопасность являются двумя сторонами одного и того же явления. Свойство информационной безопасности должно обеспечить доступность, целостность и конфиденциальность данных системы управления. Свойство функциональной безопасности должно обеспечить корректное выполнение функций системы управления, а при возникновении отказов перевести объект управления в так называемое безопасное состояние.

Еще одним мотивом знакомства с функциональной безопасностью является понимание процесса сертификации и лицензирования. Объекты, которыми управляют компьютерные системы, зачастую создают риски для окружающей среды и людей (химическое производство, газовая и нефтяная промышленность, медицинские устройства, атомные и другие электростанции, железнодорожный, автомобильный, авиационный транспорт и т.д.). Компьютерные системы управления такими объектами должны выполнять функции безопасности и обладать определенными характеристиками (резервирование, отказоустойчивость, самодиагностика, устойчивость к внешним экстремальным воздействиям и т.п.). Контроль за разработкой, внедрением и эксплуатацией компьютерных систем управления, важных для безопасности, осуществляется государственными органами сертификации и лицензирования. Таким образом, разработчикам систем приходится знакомиться с требованиями к функциональной безопасности.

1.5. Архитектура систем управления

К какому классу компьютерных систем может быть применено понятие функциональной безопасности? Очевидно, что это системы контроля и

управления. Контроль или мониторинг может быть отнесен к частному случаю управления (сбор данных с выдачей управляющего воздействия только в случае обнаружения критического отказа), поэтому будем называть такие системы просто системами управления.

Для обобщения взглянем на очевидную структуру идеального контура управления.

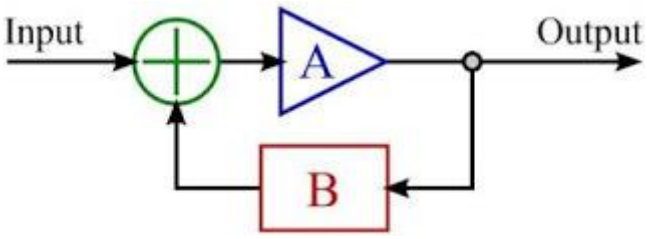

Рисунок 2.1 – Структура контура управления.

В этом контуре мы имеем: управляемый процесс, датчик, контроллер и исполнительный механизм. Необязательной с точки зрения управления, но, тем не менее, неотъемлемой частью сегодняшних систем управления являются человеко-машинный интерфейс и обработчики данных, полученных в результате мониторинга.

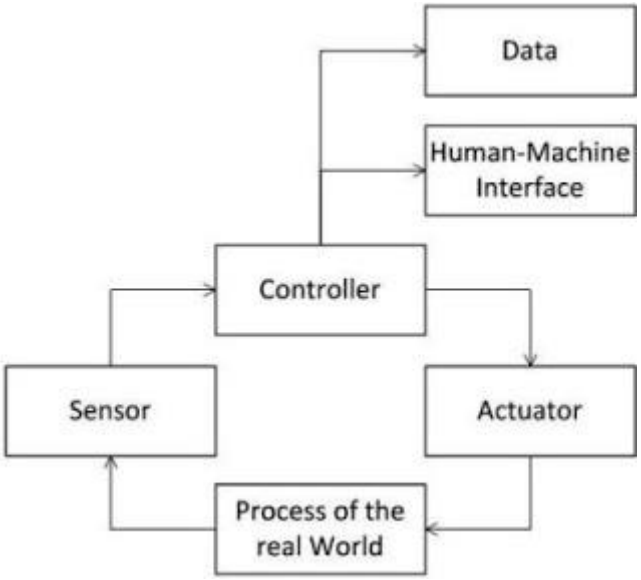

Рисунок 2.2 – Принципиальная архитектура системы управления

Подобная архитектура реализуется для встроенных систем (Embedded Systems), широко применяемых в промышленной автоматизации, бытовых устройствах, автомобильных системах, медицинских устройствах, коммуникационных сетях, роботах, дронах и т.п.

В АСУ ТП (Industrial Control Systems) применяется более разветвленная архитектура, включающая объединенные в сеть датчики, программируемые логические контроллеры (ПЛК), исполнительные механизмы, хранилища данных, сервера и рабочие станции.

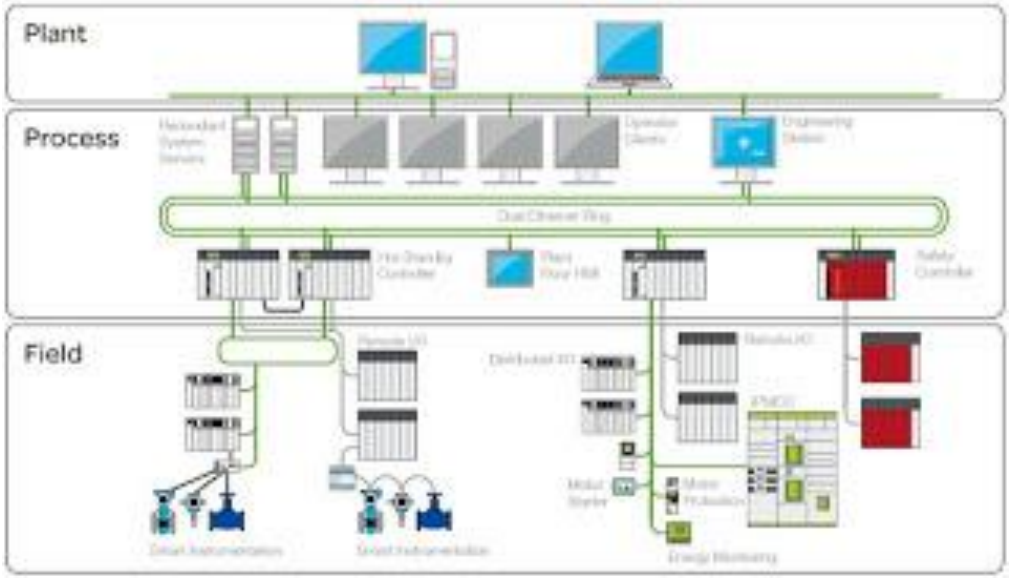

Рисунок 2.3 – Разветвленная структура системы управления.

Наиболее сложной является типовая архитектура IoT.

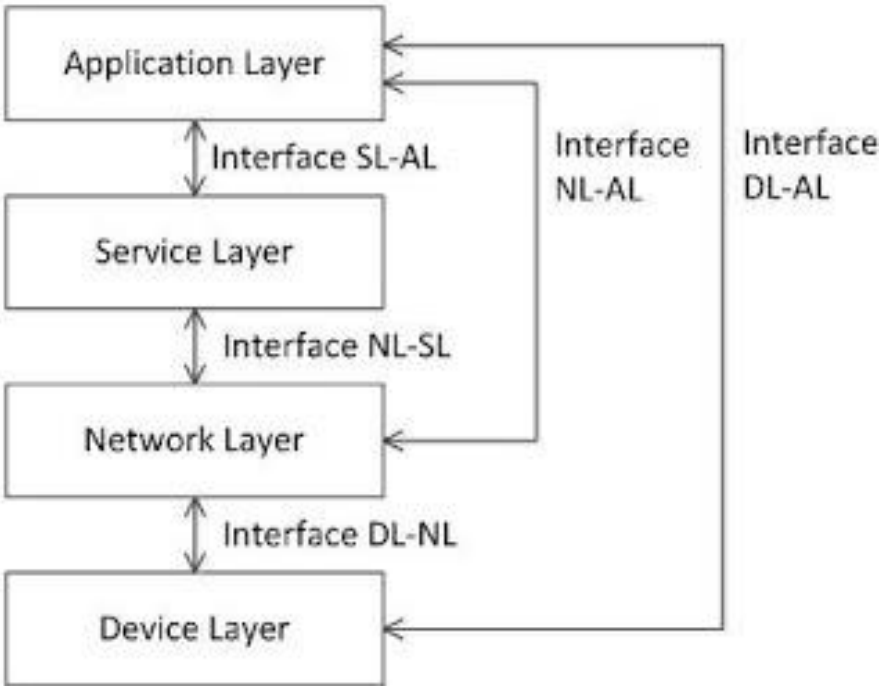

Рисунок 2.3 Типовая архитектура интернета вещей.

Управляющая система реализуется на уровне Device Layer. Ее программно-аппаратная реализация может быть аналогична встроенной системе. С точки зрения информационной безопасности критическими являются интерфейсы DL-NL & DL-AL доступа к уровню Device Layer.

Таким образом, к системам управления, для которых важно рассматривать свойство функциональной безопасности, относятся АСУ ТП, встроенные системы и IoT.

1.6. Функционально-ориентированные информационные ресурсы информационно-управляющих систем

Текст взят из источника: Чукляев И.И. Композиционная модель и способ построения функционально-ориентированных информационных ресурсов информационно-управляющих систем. Труды ИСП РАН, 2016, том 28, выпуск 2, с. 259-270.

http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=tisp&paperid=33&option_lang=rus

Интеграция информационно-телекоммуникационных технологий в сложных организационно-технических системах (ОТС) специального назначения актуализирует вопросы обеспечения их защищенности от несанкционированных внешних и/или внутренних воздействий дестабилизирующего характера (НСВ), заключающихся в разрушении, повреждении компонентов, модификации (искажении) данных ([1]), ведущих к нарушению выполнения задач управления. В настоящее время предложены разнообразные методы и средства обеспечения защищенности ОТС и циркулирующих данных в условиях НСВ. Однако, как правило, они «локализованы» относительно отдельных совокупностей данных и процессов и не ориентированы на комплексную защиту выполнения задач с учетом уровней управления ОТС [2, 3]. Предлагается композиционная модель функционально-ориентированных информационных ресурсов (ФОИР) информационно-управляющих систем (ИУС), которая отображает структуру, взаимосвязи, а также специфику операций манипулирования и обработки функционального комплекса данных на различных уровнях управления информационно-управляющих систем, соответствующего модели данных в не первой нормальной форме (non-first normal form – NFNF). Предлагаемая модель и способ построения композиционной модели ФОИР ИУС обеспечивают расширенные возможности по созданию перспективных средств защиты ИУС, ориентированных на комплексную защиту выполнения задач с учетом уровней иерархии ОТС.

Информационно-управляющая система включает функциональную, информационную, организационную и техническую подсистемы. Компоненты этих подсистем распределены по уровням управления ИУС.

1.7. Стандарты, относящиеся к функциональной

безопасности

В области стандартизации существует такое понятие, как “umbrella standard”, т.е. основополагающий «вертикальный» стандарт верхнего уровня. Для функциональной безопасности таковым является МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью» (IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems), включающий семь частей. Данный стандарт переведен на русский язык и внедрен в Российской Федерации в виде ГОСТа.

Они, скажем так, неидеальны, однако, здравый смысл в них имеется.

Согласно положениям МЭК 61508, под функциональной безопасностью (functional safety) подразумевается корректное функционирование как системы управления, так и управляемого ею оборудования. Таким образом, для обеспечения функциональной безопасности необходимо сначала определить функции безопасности (safety functions), необходимые для снижения риска управляемого оборудования, а также для достижения и сохранения этим оборудованием безопасного состояния (например, функции противоаварийной защиты). Далее, система управления должна обладать свойством так называемой полноты безопасности (safety integrity), под которым МЭК 61508 подразумевает вероятность того, что система будет корректно выполнять функции безопасности при всех заданных условиях в течение заданного интервала времени.

При обеспечении полноты безопасности (safety integrity) учитываются два типа отказов: случайные (random failures) и систематические (systematic failures).

Случайные отказы вызваны выходом из строя аппаратных компонентов и парируются такими методами, как резервирование, самодиагностика, физическое и электрическое разделение компонентов, повышение

устойчивости к внешним воздействиям и т.п.

Систематические отказы вызваны ошибками проектирования, в том числе, и ошибками программного обеспечения. Устранение систематических отказов возможно путем совершенствования процессов проектирования и разработки, тестирования, управления конфигурацией, проектного менеджмента и т.п. Кроме того, поскольку классическое резервирование не позволяет избежать систематических отказов, применяется так называемое диверсное (diversity) резервирование, когда резервные каналы разработаны с применением различного программного и аппаратного обеспечения. Дорого, неудобно, но иногда помогает.

Положения МЭК 61508 детализированы для потенциально опасных областей. Существуют, например, следующие стандарты:

— IEC 61511, Functional safety – Safety instrumented systems for the process industry sector;

— IEC 62061, Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems;

— IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety;

— ISO 26262, Road vehicles – Functional safety;
— EN 50129, Railway Industry Specific – System Safety in Electronic Systems;
— IEC 62304, Medical Device Software.

В аэрокосмической отрасли на МЭК 61508 не ссылаются, тем не менее, подход похожий:

— для авионики разработан стандарт RTCA DO-178C, Software Considerations in Airborne Systems and Equipment Certification;

— в космической отрасли стандарты разрабатываются космическими агентствами, например, NASA использует стандарт STD 8719.13, Software Safety Standard.

1.8. Соотношений функциональной и информационной безопасности

В дружной, но непредсказуемой семье «безопасность», борющейся за свободу информационных технологий от неприемлемых рисков, живут себе две сестры: старшая, функциональная безопасность (safety), и младшая, информационная безопасность (security).

Для управляющих систем, к которым относятся такие архитектуры, как АСУТП, встроенные системы и интернет вещей (Device Layer), основополагающим свойством является функциональная безопасность. Под функциональной безопасностью подразумевается корректное функционирование как системы управления, так и управляемого ею оборудования.

Информационная безопасность в таких системах носит дополнительный характер и должна предотвращать доступ злоумышленников к контролю над системой управления и управляемым оборудованием.

Подробнее: https://www.securitylab.ru/analytics/486106.php

2. ЗАЩИТА ИНФОРМАЦИИ В ИУС

3.1. Необходимость защиты информации в информационно-управляющей системе

Источник; © Национальный Открытый Университет "ИНТУИТ", 2018 | www.intuit.ru

Существование и развитие информационного общества на современном этапе невозможно без использования информационных сетей, глобальных компьютерных сетей и сетей связи — радио, телевидения, фиксированных и мобильных телефонных сетей, *Internet* и т.д. В связи с этим обеспечение доверия и безопасности невозможно без предъявления к этим сетям не только

требований по обеспечению надёжности передачи данных, стабильности работы, качества и масштабов охвата, но и по обеспечению информационной безопасности.

Информационная *безопасность* сетей представляет собой "состояние защищённости сбалансированных интересов производителей информационно-коммуникационных технологий и конкретно сетей, потребителей, операторов и органов государственной власти в информационной сфере. В свою *очередь* информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования отношений, возникающих при использовании сетей связи" [материалы Международного конгресса "*Доверие* и *безопасность* в информационном обществе", http://www.rans.ru/arrangements/int_cong_doc.doc].

Благодаря своей открытости и общедоступности *компьютерные сети* и сети связи общего пользования являются удобным средством для обеспечения взаимодействия граждан, бизнеса и органов государственной власти. Однако чем более открыты сети, тем более они уязвимы. Можно выделить ряд особенностей, которые делают сети уязвимыми, а нарушителей — практически неуловимыми:

- возможность действия нарушителей на расстоянии в сочетании с возможностью сокрытия своих истинных персональных данных (указанная особенность характерна, в частности, для сети Internet, радиосетей, сетей кабельного телевидения, незаконного использования ресурсов телефонных сетей);
- возможность пропаганды и распространения средств нарушения сетевой безопасности (например, распространение в Internet программных средств, позволяющих реализовывать несанкционированный доступ к информационным ресурсам, нарушать авторские права и т.д.);

- возможность многократного повторения атакующих сеть воздействий (например, генерация в Internet или телефонных сетях потоков вызовов, приводящих к нарушению функционирования узлов сети).

Большинство владельцев и операторов принимают необходимые меры по обеспечению информационной безопасности своих сетей. В то же время, для современного состояния информационной безопасности сетей характерны следующие причины, приводящие к крупным проблемам, требующим скорейшего решения:

- использование несогласованных методов обеспечения информационной безопасности для разных компонентов сети, включая телекоммуникационные протоколы, информационные ресурсы и приложения;
- широкое использование технических средств импортного производства, потенциально имеющих не декларированные возможности ("закладки");
- отсутствие комплексных решений по обеспечению информационной безопасности при интеграции и взаимодействии сетей;
- недостаточная проработка методологии документирования функционирования сетей, необходимого для создания доказательной базы правонарушений;
- широко распространённое отношение к обеспечению информационной безопасности как к товару или услуге, которые можно купить, а не как к процессу, который нужно не только создать, но который нужно внедрить в постоянное использование и которым необходимо постоянно управлять.

Наиболее часто встречающиеся дефекты защиты, отмеченные компаниями, работающими в области электронного бизнеса и защиты информации:

- общие проблемы в брандмауэрах, операционных системах, сетях и стандартных приложениях;
- неопознанные машины или приложения в сети;

- использование старых версий программного обеспечения на машинах сети;
- неполная информация обо всех точках входа в сеть из внешней среды;
- неполное изъятие прав доступа при увольнении сотрудников, наличие идентификаторов пользователей, используемых по умолчанию, неверно обслуживаемые права доступа;
- неоправданно открытые порты в брандмауэрах;
- необоснованный общий доступ к файловым системам;
- недостаточные требования к идентификации пользователя, собирающегося изменить регистрационные записи пользователей;
- присутствие ненужных сервисов или приложений на машинах, требующих высокой степени защиты;
- использование слабозащищенных установочных параметров, присваиваемых по умолчанию при инсталляции приложений, ввиду чего становятся известны идентификаторы и пароли пользователей, установленные по умолчанию;
- отсутствие защиты от взаимодействия внутреннего и внешнего трафика сети;
- отсутствие проверок после внесения изменений в среду (например, после инсталляции новых приложений или машин);
- отсутствие контроля вносимых изменений;
- отсутствие информации о внутренних угрозах безопасности;
- отсутствие информации о слабых местах различных методик аутентификации при организации мощной защиты.

Любая успешная *атака* нарушителя, направленная на реализацию угрозы информационной безопасности сети, опирается на полученные нарушителем знания об особенностях её построения и слабых местах. Причинами появления уязвимостей в сетях могут быть:

- уязвимые зоны в поставляемом программном продукте;
- нарушение технологий передачи информации и управления;

- внедрение компонентов и программ, реализующих не декларированные функции и нарушающих нормальное функционирование сетей;
- невыполнение реализованными механизмами защиты сети заданных требований к процессу обеспечения информационной безопасности или предъявление непродуманного набора требований;
- использование не сертифицированных в соответствии с требованиями безопасности отечественных и зарубежных информационных технологий, средств информатизации и связи, а также средств защиты информации и контроля их эффективности.

Постоянный *аудит* сетей связи с целью выявления уязвимостей и возможных угроз обеспечивает *определение* "слабого звена", а уровень защищённости "слабого звена" определяет, в конечном счёте, уровень информационной безопасности сети в целом.

Принципиальным является рассмотрение воздействий нарушителей или атак как неизбежного фактора функционирования сетей и систем связи. Это обстоятельство является обратной стороной информатизации экономики и бизнеса.

В этих условиях обеспечение информационной безопасности сетей становится триединой задачей, включающей *мониторинг* функционирования, обнаружение атак и принятие адекватных мер противодействия.

Адекватные меры противодействия могут носить технический характер и предусматривать реконфигурацию информационной области сети. Они могут быть также организационными и предусматривать обращение операторов сетей связи к силовым структурам с предоставлением необходимой информации для выявления и привлечения к ответственности нарушителей.

Обеспечение информационной безопасности сетей, систем и средств связи означает *создание процесса*, которым необходимо постоянно управлять и который является неотъемлемой составной частью процесса

функционирования компьютерных вычислительных устройств и сетей. Построив модель функционирования сети, включающую *процесс управления* обеспечением информационной безопасности, необходимо далее определить стандарты информационной безопасности, поддерживающие эту модель. *Значение* исследований процессов стандартизации и совершенствования нормативно-правовой базы будут постоянно возрастать.

Вопросы информационной безопасности, защиты информации и данных неразрывно связаны с безопасностью программно-аппаратных комплексов и сетевых устройств, образующих *информационно-управляющие системы* и сети различного назначения. Такие системы должны отвечать серьёзным требованиям по обеспечению надёжности сбора, обработки, архивирования и передачи данных по открытым и закрытым сетям и обеспечению их максимальной защиты.

3.2. Определение защищенной информационно-управляющей системы

В отличие от локальных корпоративных сетей, подключенных к Internet, где обычные средства безопасности в большой степени решают проблемы защиты внутренних сегментов сети от несанкционированного доступа, информационно-управляющие системы предъявляют повышенные требования в плане обеспечения информационной безопасности.

Межсетевые экраны, системы обнаружения атак, сканеры для выявления уязвимостей в узлах сети, операционных систем и СУБД, фильтры пакетов данных на маршрутизаторах — достаточно ли всего этого мощного арсенала (так называемого «жёсткого периметра») для обеспечения безопасности критически важных информационнно-управляющих систем, работающих в Internet и Intranet? Практика и накопленный к настоящему времени опыт показывают — чаще всего нет!

В «Оранжевой книге» надежная и защищённая информационная

система определяется как «система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную достоверную обработку информации разной степени секретности различными пользователями или группами пользователей без нарушения прав доступа, целостности и конфиденциальности данных и информации, и поддерживающая свою работоспособность в условиях воздействия на неё совокупности внешних и внутренних угроз» [Department of Defense Trusted Computer System Evaliation Criteria (TCSEC). USA DoD 5200.28-STD, 1993].

Это качественное определение содержит необходимое и достаточное условие безопасности. При этом не обуславливается, какие механизмы и каким образом реализуют безопасность — практическая реализация зависит от многих факторов: вида и размера бизнеса, предметной области деятельности компании, типа информационной системы, степени её распределённости и сложности, топологии сетей, используемого программного обеспечения и т.д.

Концепция «Защищенные информационные системы» включает ряд законодательных инициатив, научных, технических и технологических решений, готовность государственных организаций и компаний использовать их для того, чтобы люди, используя устройства на базе компьютеров и программного обеспечения, чувствовали себя так же комфортно и безопасно. В общем случае можно говорить о степени доверия, или надежности систем, оцениваемых по двум основным критериям: наличие и полнота политики безопасности и гарантированность безопасности.

Наличие и полнота политики безопасности — набор внешних и корпоративных стандартов, правил и норм поведения, отвечающих законодательным актам страны и определяющих, как организация собирает, обрабатывает, распространяет и защищает информацию. В частности, стандарты и правила определяют, в каких случаях и каким образом пользователь имеет право оперировать с определенными наборами данных. В

политике безопасности сформулированы права и ответственности пользователей и персонала. В зависимости от сформулированной политики можно выбирать конкретные механизмы, обеспечивающие безопасность системы. Чем больше информационная система и чем больше она имеет «входов» и «выходов» (распределённая система), тем «строже», детализированнее и многообразнее должна быть политика безопасности.

Гарантированность безопасности — мера доверия, которая может быть оказана архитектуре, инфраструктуре, программно-аппаратной реализации системы и методам управления её конфигурацией и целостностью. Гарантированность может проистекать как из тестирования и верификации, так и из проверки (системной или эксплуатационной) общего замысла и исполнения системы в целом и ее компонентов. Гарантированность показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности. Гарантированность является пассивным, но очень важным компонентом защиты, реализованным качеством разработки, внедрения, эксплуатации и сопровождения информационно-управляющей системы и заложенных принципов безопасности.

Концепция гарантированности является центральной при оценке степени, с которой информационно-управляющую систему можно считать надежной. Надежность определяется всей совокупностью защитных механизмов системы в целом и надежностью вычислительной базы (ядра системы), отвечающих за проведение в жизнь политики безопасности. Надежность вычислительной базы определяется ее реализацией и корректностью исходных данных, вводимых административным и операционным персоналом. Оценка уровня защищенности ИТ/ИС обычно производится по трём базовым группам критериев (таблица 3.1).

Таблица 3.1. Трёхуровневая модель параметров оценки защищенности ИС

Система целей	**Средства**	**Исполнение**

Общая цель	Обеспечение	Установки
Защищенные информационно-управляющие системы	Защищенность	Законы, нормы
	Конфиденциальность	Характер ведения бизнеса
	Целостность	Контракты, обязательства
Цели	Готовность к работе	Внутренние принципы
Безопасность	Точность	Международные, отраслевые, и внутренние стандарты
Безотказность	Управляемость	
Надежность	Безотказность	
Деловое взаимодействие	Прозрачность	Реализация
	Удобство пользования	Методы взаимодействия с внешней и внутренней средой
	Подтверждение доверия	Методы работ
	Внутренняя оценка	Анализ рисков
	Аккредитация	Методы разработки, внедрения, эксплуатации и сопровождения
	Внешний аудит	Обучение персонала

Основное назначение надежной вычислительной базы — выполнять функции монитора обращений и действий, то есть контролировать допустимость выполнения пользователями определенных операций над объектами. Монитор проверяет каждое обращение к программам или данным на предмет их согласованности со списком допустимых действий. Таким образом, важным средством обеспечения безопасности является механизм подотчетности или протоколирования. Надежная система должна фиксировать все события, касающиеся безопасности, а ведение протоколов дополняется аудитом — анализом регистрационной информации.

Эти общие положения являются основой для проектирования и

реализации безопасности информационно-управляющих систем.

3.3. Стандарты информационной безопасности

Текст взят из открытого источника https://arinteg.ru/articles/standarty-informatsionnoy-bezopasnosti-27697.html.

Стандарты информационной безопасности – это обязательные или рекомендуемые к выполнению документы, в которых определены подходы к оценке уровня информационной безопасности и установлены требования к безопасным информационным системам.

Стандарты в области информационной безопасности выполняют следующие важнейшие функции:

- выработка понятийного аппарата и терминологии в области информационной безопасности,
- формирование шкалы измерений уровня информационной безопасности,
- согласованная оценка продуктов, обеспечивающих информационную безопасность,
- повышение технической и информационной совместимости продуктов, обеспечивающих ИБ,
- накопление сведений о лучших практиках обеспечения информационной безопасности и их предоставление различным группам заинтересованной аудитории – производителям средств ИБ, экспертам, ИТ-директорам, администраторам и пользователям информационных систем,
- функция нормотворчества – придание некоторым стандартам юридической силы и установление требования их обязательного выполнения.

Благодаря стандартам информационной безопасности производители и эксперты обоснованно определяют наборы требований к информационным системам и декларируют их возможности и подтверждают ценности продукции путем сертификации на соответствие стандартам информационной

безопасности.

С другой стороны, благодаря стандартам информационной безопасности потребители обоснованно выбирают информационные системы, четко формулируют требования к ним и имеют возможность построить гарантированно качественную систему информационной безопасности.

Согласно Федеральному закону №184-ФЗ «О техническом регулировании», целями стандартизации являются:

- повышение уровня безопасности жизни и здоровья граждан, имущества физических и юридических лиц, государственного и муниципального имущества, объектов с учетом риска возникновения чрезвычайных ситуаций природного и техногенного характера, повышение уровня экологической безопасности, безопасности жизни и здоровья животных и растений;
- обеспечение конкурентоспособности и качества продукции (работ, услуг), единства измерений, рационального использования ресурсов, - взаимозаменяемости технических средств (машин и оборудования, их составных частей, комплектующих изделий и материалов), технической и информационной совместимости, сопоставимости результатов исследований (испытаний) и измерений, технических и экономико-статистических данных, проведения анализа характеристик продукции (работ, услуг), исполнения государственных заказов, добровольного подтверждения соответствия продукции (работ, услуг);
- содействие соблюдению требований технических регламентов;
- создание систем классификации и кодирования технико-экономической и социальной информации, систем каталогизации продукции (работ, услуг), систем обеспечения качества продукции (работ, услуг), систем поиска и передачи данных, содействие проведению работ по унификации.

Основными областями стандартизации информационной безопасности являются:

- аудит информационной безопасности,
- модели информационной безопасности,
- методы и механизмы обеспечения информационной безопасности,
- криптография,
- безопасность межсетевых взаимодействий,
- управление информационной безопасностью.

Стандарты информационной безопасности имеют несколько классификаций.

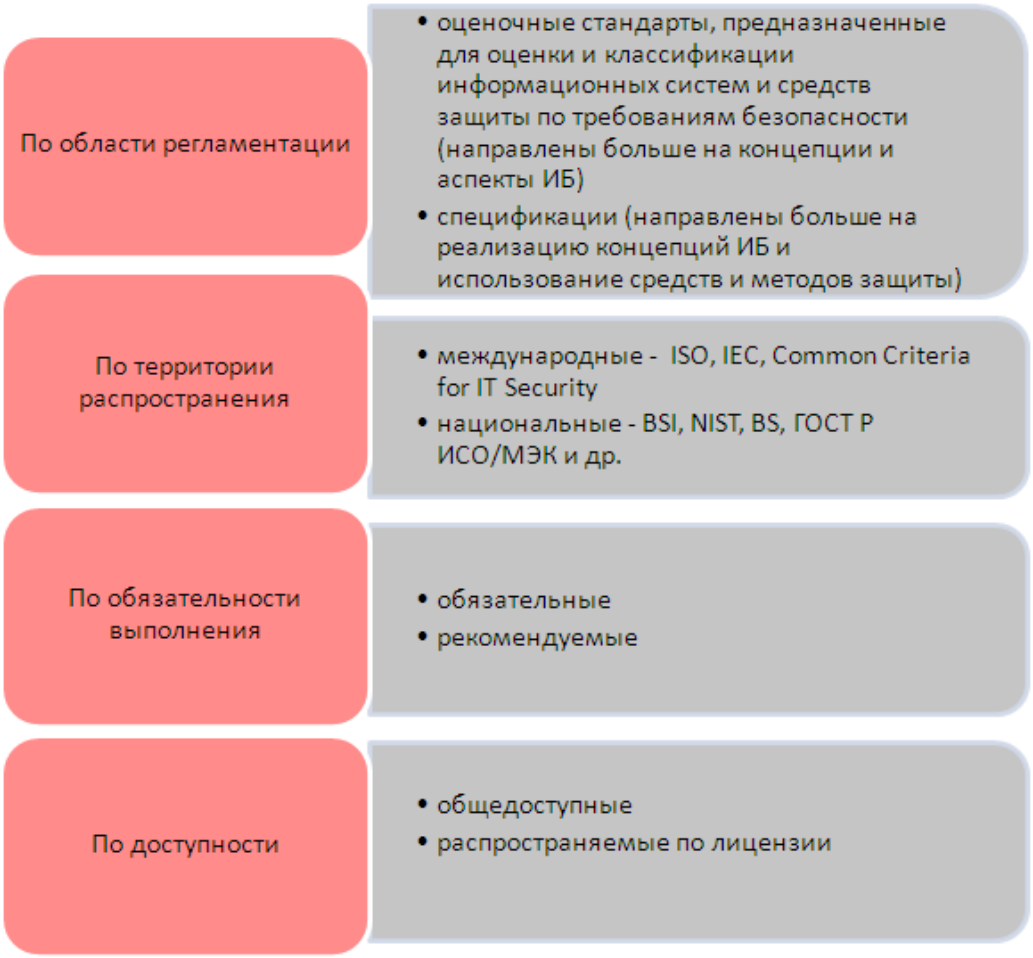

Рисунок 3.1 – Классификация стандартов информационной безопасности.

Существуют российские стандарты информационной безопасности (ГОСТ Р ИСО/МЭК 15408, ГОСТ Р 51275 и др.), причем Федеральный закон

№184-ФЗ «О техническом регулировании» декларирует принцип «применения международного стандарта как основы разработки национального стандарта, за исключением случаев, если такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и (или) технологическим особенностям или по иным основаниям, либо Российская Федерация в соответствии с установленными процедурами выступала против принятия международного стандарта или отдельного его положения».

Необходимость следования некоторым стандартам информационной безопасности закреплена законодательно.

3.4. Методология анализа защищенности информационной системы

При разработке архитектуры и создании инфраструктуры корпоративной ИС неизбежно встает вопрос о её защищенности от угроз. Решение вопроса состоит в подробном анализе таких взаимно пересекающихся видов работ, как реализация ИС и её аттестация, аудит и обследование безопасности ИС.

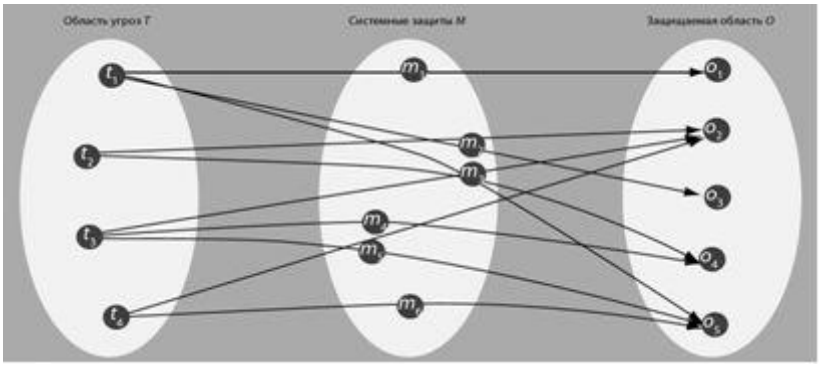

Рисунок 3.1. Модель системы защиты с полным перекрытием

Основой формального описания систем защиты традиционно считается

модель системы защиты с полным перекрытием (рис. 5.1), в которой рассматривается взаимодействие "области угроз", "защищаемой области" и "системы защиты". Таким образом, имеем три множества: $T = {}_t i$ — множество угроз безопасности, $O = o_j$ — множество объектов (ресурсов) защищенной системы, $M = m_k$ — множество механизмов безопасности АС.

Элементы этих множеств находятся между собой в определенных отношениях, собственно и описывающих систему защиты. Для описания системы защиты обычно используется графовая модель. Множество отношений угроза-объект образует двухдольный граф T, O. Цель защиты состоит в том, чтобы перекрыть все возможные ребра в графе. Это достигается введением третьего набора M; в результате получается трехдольный граф T, M, O.

Развитие модели предполагает введение еще двух элементов (рис. 5.2). Здесь V — набор уязвимых мест, определяемый подмножеством декартова произведения $T * O : v_r =< t_i, o_j >$. Под уязвимостью системы защиты понимают возможность осуществления угрозы T в отношении объекта O. (На практике под уязвимостью системы защиты обычно понимают, те свойства системы, которые либо способствуют успешному осуществлению угрозы, либо могут быть использованы злоумышленником для её осуществления).

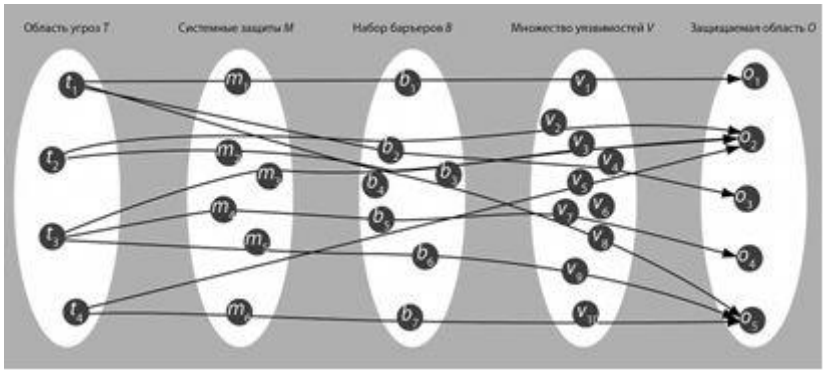

Рисунок 3.2. Модель системы защиты, содержащей уязвимости

Определим B как набор барьеров, определяемый декартовым произведением, представляющих собой пут $V * M : b_l =< t_i, o_j, m_k >$ и осуществления угроз безопасности, перекрытые средствами защиты. В результате получаем систему, состоящую из пяти элементов: $< T, O, M, V, B >$, описывающую систему защиты с учетом наличия уязвимостей.

Для системы с полным перекрытием для любой уязвимости имеется устраняющий ее барьер. Иными словами, в подобной системе защиты для всех возможных угроз безопасности существуют механизмы защиты, препятствующие осуществлению этих угроз. Данное условие является первым фактором, определяющим защищенность ИС, второй фактор — "прочность" и надёжность механизмов защиты.

В идеале каждый механизм защиты должен исключать соответствующий путь реализации угрозы. В действительности же механизмы защиты обеспечивают лишь определённую степень сопротивляемости угрозам безопасности. Поэтому в качестве характеристик элемента набора барьеров $b_l =< t_i, o_j, m_k >$ может рассматриваться набор $< P_l, L_l, R_l >$, где P_l — вероятность появления угрозы, L_l — величина ущерба при удачном осуществлении угрозы в отношении защищаемых объектов (уровень серьезности угрозы), а R_l — степень сопротивляемости механизма защиты m_k, характеризующаяся вероятностью его преодоления.

Надёжность барьера $b_l =< t_i, o_j, m_k >$ характеризуется величиной остаточного риска $Risk_l$, связанного с возможностью осуществления угрозы t_i в отношении объекта информационной системы o_j при

использовании механизма защиты mk. Эта величина определяется по формуле: $Risk_l = P_k * L_k * (1-R_k)$. Для нахождения примерной величины защищенности S можно использовать следующую простую формулу: $S = 1/Risk_0$, где $Risk_0$ является суммой всех остаточных рисков, $(0 < [P_k, L_k] < 1)$, $(0 \leq R_k < 1)$.

Суммарная величина остаточных рисков характеризует приблизительную совокупную уязвимость системы защиты, а защищенность определяется как величина, обратная уязвимости. При отсутствии в системе барьеров b_k, "перекрывающих" выявленные уязвимости, степень сопротивляемости механизма защиты R_k принимается равной нулю.

На практике получение точных значений приведенных характеристик барьеров затруднено, поскольку понятия угрозы, ущерба и сопротивляемости механизма защиты трудно формализовать. Так, оценку ущерба в результате несанкционированного доступа к информации политического и военного характера точно определить вообще невозможно, а определение вероятности осуществления угрозы не может базироваться на статистическом анализе. Построение моделей системы защиты и анализ их свойств составляют предмет "теории безопасных систем", еще только оформляющейся в качестве самостоятельного направления.

Вместе с тем, для защиты информации экономического характера, допускающей оценку ущерба, разработаны стоимостные методы оценки эффективности средств защиты. Для этих методов набор характеристик барьера дополняет величина C_l затраты на построение средства защиты барьера b_l. В этом случае выбор оптимального набора средств защиты связан с минимизацией суммарных затрат $W = w_l$, состоящих из затрат $C = c_l$ на создание средств защиты и возможных затрат в результате успешного осуществления угроз $N = n_l$.

Формальные подходы к решению задачи оценки защищенности из-за трудностей, связанных с формализацией, широкого практического распространения не получили. Значительно более действенным является использование неформальных классификационных подходов. Для этого применяют категорирование: нарушителей (по целям, квалификации и доступным вычислительным ресурсам); информации (по уровням критичности и конфиденциальности); средств защиты (по функциональности и гарантированности реализуемых возможностей), эффективности и рентабельности средств защиты и т. п.

3.5. Безопасность промышленных систем автоматизации и управления

Промышленные системы автоматизации и управления являются основными компонентами инфраструктуры современных предприятий, принадлежащим к различным секторам экономики (топливно-энергетический комплекс, металлургическая промышленность, химическая промышленность и др.) и могут включать в себя системы управления производственными процессами (MES), системы диспетчерского управления и сбора данных (SCADA), системы управления, построенные на базе программируемых логических контроллеров (PLC), и др. Обеспечение информационной безопасности промышленных систем автоматизации и управления как критически важных элементов бизнес-процессов, является неотъемлемой частью процесса обеспечения безопасности предприятия в целом.

В настоящее время, при развитии и модернизации предприятий, в промышленных системах внедряются унифицированные технологии (IP/Ethernet), новые сервисы (Виртуализация, IP-телефония, Мобильность и др.), повышается уровень автоматизации технологических процессов и осуществляется интеграция с системами управления предприятием (ERP). В

свою очередь, повышение уровня автоматизации может привести и к увеличению вероятности реализации известных угроз, и к появлению новых угроз безопасности.

Важно отметить, что, в течение последних десяти лет, наблюдается значительный рост количества инцидентов и выявленных уязвимостей, а также целенаправленных атак на промышленные системы автоматизации и управления, целью которых являются промышленный шпионаж, мошенничество и нарушение функционирования предприятия.

Обеспечение безопасности промышленных систем автоматизации и управления — сложная задача, требующая комплексного подхода, для решения которой необходимо учитывать и специфику промышленных систем (в том числе, и использование устаревших и уязвимых компонентов, протоколов, требования к надежности и непрерывности функционирования, климатические условия и др.), международные стандарты и лучшие практики (IEC 62443 (ISA 99), CIP NERC, NIST и др.), требования регулирующих органов РФ, направленные на повышение безопасности ключевых систем информационной инфраструктуры (КСИИ): 256-ФЗ «О безопасности объектов ТЭК», документ Совета Безопасности, документы ФСБ России и ФСТЭК России. В рамках комплексного подхода по обеспечению безопасности промышленных систем автоматизации и управления решаются задачи защиты обрабатываемой информации, обеспечения непрерывности функционирования технологических процессов, а также противодействие мошенничествам и хищению.

Меры по обеспечению безопасности промышленных систем автоматизации и управления:

- аудит промышленных систем автоматизации и управления, включающий в себя идентификацию и классификацию активов, проведение тестов на проникновение, проведение анализа истории инцидентов, оценку рисков, разработку стратегии развития системы безопасности;

- создание комплексного решения по обеспечению безопасности промышленных систем автоматизации и управления, включая работы по обследованию, построению модели угроз и оценки рисков, формированию требований, с учетом международных стандартов и лучших практик, разработку проектной и рабочей документации, ввод в действие комплексной системы безопасности;
- сервисная поддержка, включающая в себя комплекс действий по техническому сопровождению систем безопасности.

3.6. Методы и средства защиты информационно-управляющих систем от помех в сетях электропитания

Текст взят из работы: Юрин Сергей Юрьевич. Методы и средства защиты информационно-управляющих систем от помех в сетях электропитания. Автореферат диссертации на соискание ученой степени к.т.н. Специальность 05.13.05

Обеспечение высокой помехоустойчивости средств вычислительной техники (СВТ), входящих в состав информационно-управляющих систем (ИУС), - одна из основных проблем, решаемых разработчиками. Рост энерговооруженности производства, увеличение уровня возникающих помех, с одной стороны, и повышение степени интеграции электронных средств и снижение энергетической мощности полезных сигналов, с другой стороны, приводит к тому, что полезные сигналы на фоне действующих помех подвержены искажению, поэтому защита полезного сигнала является весьма актуальной.

Работа управляющих устройств в составе киберфизических систем связана с неизбежным возникновением мощных помех, специфика которых определяется их незначительной частотой появления и узким собственным частотным диапазоном. Особую острогу проблема борьбы с помехами в сетях электропитания приобретает в промышленных условиях. Это связано с

наличием большого количества перемещающихся двигателей, мощных реле и переключателей.

Проблема обеспечения надежности и устойчивости работы ИУС в условиях многочисленных, разнообразных по физической природе, частотным характеристикам и энергетическому спектру помех, является актуальной и своевременной задачей, для решения которой требуется разработка специальных устройств для контроля уровня помех и разработка рекомендаций по построению помехозащищенных ИУС.

Наиболее опасными для СВТ и часто встречающимися видами помех следует отнести импульсные помехи и кратковременные провалы напряжения в сетях электропитания. Поэтому задачи контроля уровня импульсных помех и защиты от кратковременных провалов напряжения являются актуальными и требуют разработки специальных устройств. Помехи в системе управления вызывают сбои и искажения передаваемой информации, что приводит к ухудшению экономико- технологических показателей. Недостаточная или чрезмерная защита от помех может привести к потере прибыли производством. Поэтому следует решить задачу оптимизации средств защиты ИУС от помех в промышленных сетях питания по экономическому критерию. В связи с тем. что в настоящее время основу ИУС составляют персональные компьютеры (ПК), то целесообразно при решении поставленных задач использовать периферийные устройства ПК.

Для повышения помехозащищенности информационно- управляющих необходимо решить следующие задачи:

- исследование импульсных помех и кратковременных провалов напряжения в сетях электропитания;
- разработка системы выбора средств и методов защиты ИУС от помех по сетям электропитания;
- разработка аппаратно-программных комплексов на базе персонального компьютера для экспресс-анализа уровня импульсных помех и

прогнозирования кратковременных провалов напряжения в промышленной сети питания;

- разработка рекомендаций по построению помехозащищенных информационно-управляющих систем.

Основным методом экспериментальных исследований является физическое макетирование аппаратно-программных комплексов на основе ПК для экспресс-анализа уровня импульсных помех и прогнозирования кратковременных провалов напряжения в промышленной сети питания, разработка системы выбора средств и методов защиты ИУС от помех по сетям электропитания, а также имитационное моделирование по исследованию методических погрешностей экспресс-анализа уровня импульсных помех в сети электропитания.

5. ПОМЕХИ И СБОИ МНОГОУРОВНЕВЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

5.1. Анализ существующих методов и средств защиты многоуровневых ИУС от помех

Виды и параметры импульсных и длительных помех, источники и пути их проникновения, а также последствия, вызываемые воздействием помех на СВТ систем управления - все это определяет методы защиты ИУС от помех.

Универсальных методов защиты от помех не существует, так как любая сложная система с точки зрения характера помеховой обстановки и путей воздействия на нее помех является индивидуальной. Известны три основных группы (рисунок 8) борьбы с помехами: - снижение уровня (амплитуды) помех; - подавление помех общего вида; - подавление помех нормального вида. Первая группа способов предусматривает как уменьшение источников помех, так и уровня сигналов в источниках помех и способы, относящееся к этой группе, основаны на предотвращении возникновения источников помех, подавлении и компенсации помех. Эти способы хорошо изучены и широко применяются на практике [21-23, 29, 39, 57, 80, 89]. В устройствах, содержащих контакторы, реле, прерыватели и другие элементы коммутации, схемы снижения уровня помех представляют собой реактивные искрогасящие цепочки и резистивные шунты, устанавливаемые параллельно контактам. Получили широкое распространение групповые емкостные фильтры, устанавливаемые в силовых шкафах между токонесущими шинами и заземленным корпусом. Эти фильтры значительно снижают уровень помех от силового питания [21-23].

Сетевые фильтры устанавливаются в устройствах систем управления для предотвращения проникновения помех со стороны первичного питания. Такие фильтры включают также между питающей цепью и выпрямителями в

блоках стабилизированного питания для устранения внутренних источников помех в системе управления [21-23].

Одним из эффективных средств борьбы с мощными источниками помех от электротехнического оборудования является: пространственное разделение источников помех и каналов передачи сигналов и электростатическое экранирование [21-23].

Известны ряд практических рекомендация по выполнению кабельных трасс, взаимному размещению кабелей и соединительных линий каналов передачи информации, силовой проводки и электротехнического оборудования [38]. Значительное уменьшение общего уровня помех в системах управления достигается правильным выполнением заземлений в системе. Это достигается, прежде всего, тем, что для каждого оборудования на объекте создаются специальные независимые цепи заземления и выполняются все требования по заземлению устройств, соединительные цепи которых не вызывают дополнительных помех в системах передачи информации.

Электрическим цепям питания следует уделять особое внимание, так как они являются не только наиболее распространенными источниками помех, но и передатчиками помех, возникающих в технологическом оборудовании. Вторая группа способов борьбы с помехами включает в себя способы, направленные на подавление помех общего вида путем уменьшения паразитных связей источников помех с каналами: передачи информации и путем увеличения затухания сигнала помехи при проникновении в каналы передачи информации. Это достигается экранированием узлов и цепей устройств системы управления, гальваническим разделением цепей в каналах передачи информации, симметрированием цепи передачи каналов и компенсаций помех общего вида. Способы подавления помех общего вида подробно рассмотрены в работе [38].

Третья группа включает способы борьбы с помехами направленные на снижение помех нормального вида, повышение достоверности передачи

информации. При этом применяют следующие технические приемы борьбы с помехами: промежуточное усиление и преобразование сигналов в канале, параметрическая компенсация помех нормального вида, фильтрация, выделение и вычитание помехи в канале передачи сигналов, синхронное детектирование, гармонический отбор сигнала, интегрирование и усреднение, специальные способы обработки полезного сигнала с наложенной помехой. Известны эффективные аппаратные способы борьбы с помехами нормального вида, использующие кодирование сообщений и приема, а также применения пороговых схем, каналов с обратной связью и использование методов дублирования с получением результатов приема сигналов по большинству совпадений. В настоящее время программно-алгоритмические способы борьбы с помехами становятся все более перспективными, т.к. мощность современных СВТ неуклонно возрастает. Способы подавления помех нормального вида также подробно рассмотрены в работе [38]. Опыт исследований ИУС показывает, что выбор способов защиты от помех должен производится исходя из помеховой обстановки на объекте, пороговых свойств СВТ, особенностей структуры системы и ее технических характеристик, требований по надежности функционирования системы и минимальных затрат на средства защиты для достижения требуемой надежности. Анализ существующих критериев выбора средств защиты показал, что эти критерии основаны на характеристиках параметров надежности (интенсивность сбоя, вероятность сбоя и т.п.) [21, 48].

5.2. Критерий оптимизации средств защиты информационно-управляющих систем от внешних помех

Помехи в системе управления вызывают сбои и искажения передаваемой информации, что приводит к ухудшению экономико-

технологических показателей. Недостаточная или чрезмерная защита от помех может привести к потере прибыли производством. Поэтому следует решить задачу оптимизации средств защиты ИУС от помех в промышленных сетях питания по экономическому критерию.

5.3. Исследование функции нормированной годовой экономии

На основании проведенных исследовании областей существования и линий равной нормированной годовой экономии, предлагается следующая методика оптимизации средств и методов защиты ИУС от помех по сети питания.

1. Методом экспертных оценок построить зависимость затрат на различные средства подавления помех от вероятности подавления.

2. Аппроксимировать функции затрат полиномом II степени и найти значения коэффициентов полиномов.

3. Определить вид и параметры функций распределения амплитуды импульсных помех в сети питания ИУС и интенсивность следования помех.

4. Решить систему дифференциальных уравнений. Найти оптимальные коэффициенты подавления помех различными средствами защиты.

5. Если невозможно или затруднительно технически реализовать подученные коэффициенты подавления помех, построить линии равной нормированной годовой экономии.

6. Исходя из технических возможностей, выбрать коэффициенты подавления помех различными средствами защиты и разработать ТУ к используемым средствам. Необходимо отметить, что п. 1 данной методики требует достаточного времени, а для реализации п. 3 необходимо устройство экспресс-анализа импульсных помех. Промышленность серийно таких приборов не выпускает, поэтому возникает задача в разработке такой аппаратуры.

На основе анализа существующих методов защиты ИУС от внешних помех по сети питания целесообразно осуществлять защиту ИУС с учетом затрат на средства защиты от помех.

Критерий выбора средств и методов защиты ИУС от помех в сетях питания равен нормированной годовой экономии от применения средств и методов защиты ИУС от помех, и учитывает эффективность применения средств и методов защиты от помех, их стоимость, а также их вероятностные характеристики надежности.

Исследования функции нормированной годовой экономии позволяют выбрать степень полиномов, аппроксимирующих затраты на средства защиты от помех, и получить формульные соотношения определения коэффициентов ослабления амплитуды помех (для различных методов и средств защиты), в зависимости от коэффициентов аппроксимирующих полиномов.

При оптимизации средств защиты ИУС от помех необходимо знать вид и параметры закона распределения амплитуды помех в сети питания ИУС. Для их определения необходимо устройство анализа импульсных помех в сети питания. Промышленность серийно таких приборов в настоящее время не выпускает. Таким образом, возникает задача в разработке аппаратуры для анализа помех в сети питания и методики ее использования. Статистические значения плотности вероятности могут быть получены с помощью многоканальных или одноканальных дифференциальных устройств анализа. В многоканальных используются группированные выборки, так как анализ является одновременным. Теория оценивания по группированным выборкам обстоятельно рассмотрена в [55]. В одноканальных устройствах анализа, анализ является последовательным, поэтому статистические значения вероятности попадания значения случайного процесса в /-й интервал анализа определяется не как отношение числа попадания случайной величины в этот интервал к общему числу случайных величин N за все время измерения, как это делается в многоканальных устройствах анализа, а как отношение числа

попаданий случайной величины в рассматриваемый интервал к числу случайных величин и,, которые наблюдаются при определении статистических значений плотности вероятности в данном / -м интервале. Поэтому для одноканальных устройств анализа нельзя говорить о группировании данных, следовательно, нельзя использовать теорию оценивания по группированным выборкам для получения оценки и определения ее точности. Первая оценка не является состоятельной и асимптотически эффективной, нуждается во введении поправок на нелинейность методом последовательных приближений и не имеет преимуществ в легкости выполнения вычислений; поэтому выберем оценку, полученную методом максимального правдоподобия, которая является состоятельной, несмещенной и асимптотически эффективной.

5.4. Исследование законов распределения амплитуды импульсных помех

Исследования проводились в сетях питания ИУС, работающей в составе автоматизированной линии розлива пивоваренного завода «ОЧАКОВО». На исследуемом предприятии ИУС подсоединялась к общей сети питания, от которой питались также такие мощные потребители энергии, как калориферы, транспортеры, и другое оборудование. Исследование импульсных помех проводилось в месте непосредственного подключения ИУС. Изменяя уровни анализа по амплитуде, определялись статистические значения функции распределений по формуле (1.3). В каждом положении канала наблюдалось 200 импульсов. Полученные результаты (таблица 4.1), обработанные по критерию согласия %2, показали, что амплитуда импульсов помех подчиняется следующим законам распределения: экспоненциальному, сдвинутому экспоненциальному, и закону Релея. Необходимо отметить, что в ряде испытаний закон распределения с равной доверительной вероятностью

мог быть принят релеевским или логнормальным, но применение более мощного критерия W2 показало более удовлетворительную аппроксимацию релеевским законом распределения. Гистограммы распределений приведены на рисунке 32.

Исследование показало, что при непосредственном расположении ИУС с технологическим оборудованием закон распределения амплитуды является экспоненциальными, при удалении Релея, а при большем удалении от технологического оборудования и экранировании сетевого кабеля сдвинутыми экспоненциальными. То есть удаление ИУС от технологической зоны приводит к тому, что помехи малой амплитуды затухают.

Из результатов испытаний видно (таблица 4.2), что параметры законов распределений амплитуды могут изменяться в широких пределах от 10 до 50 В, а сдвиг может достигать 5... 15 В.

При сравнении частоты следования и распределения амплитуды помех положительной и отрицательной полярности существенной разницы не было отмечено (рисунок 33). Также проводились исследования потока помех. При этом использовалась методика проверки потока помех на стационарность, изложенная в [34]. То есть проводилось (10...14) реализаций функции распределения амплитуды импульсов помех. Полученные статистические значения функций распределений амплитуды импульсов и результаты обработки приведены в приложении А. Анализ результатов расчета показал, что с доверительной вероятностью, равной 0.4, можно утверждать, что исследуемый поток помех стационарный.

Таким образом, проведенные исследования импульсных помех в сети питания ИУС полностью подтвердили принятые ранее (глава 1) допущения о стационарности потока помех, статистической независимости амплитуды и длительности импульсов, о том, что амплитуда помех распределены по следующим законам: экспоненциальному, сдвинутому экспоненциальному и закону Релея.

Проведенные исследования (глава 3) показали, что наиболее оптимальной структурой аппаратно-программного комплекса на базе ПК для экспресс-анализа импульсных помех в промышленных сетях электропитания, является структура одноканального интегрального устройства анализа в режиме определения статистических значений функции распределения в одной точке.

Для подтверждения теоретических выводов, приведенных в главе 3, проведем имитационное моделирование определения методических погрешностей экспресс-анализа параметров закона распределения амплитуды импульсных помех.

На основе анализа [2, 23, 31, 34, 44, 56, 83] и полученных результатов (глава 3) разработаем аппаратно-программный комплекс на базе ПК для экспресс-анализа импульсных помех в промышленных сетях электропитания [114, 116], структурная схема которого представлена на рисунке 36.

Данный комплекс (вид программного обеспечения комплекса представлен на рисунке 37) построен на базе ПК, оснащенного звуковой картой Creative SB Live 5.1 (или выше) и TV или FM - тюнером на чипе Bt 878 (например, PixelView).

Ослабленный через делитель напряжения сигнал из сети питания подается на вход тюнера. Тюнер выступает в роли детектора, чтобы выявить высокочастотные импульсные помехи в сети питания, т.к. рабочая частота звуковой карты ограничена 48 кГц. Далее сигнал поступает на линейный вход звуковой карты и преобразуется в цифровую форму. Чтобы исключить низкочастотную составляющую сигнала, данные с АЦП карты программно обрабатываются фильтром высоких частот. В качестве реализации алгоритма фильтра используется библиотека Intel Signal Processing Library 4.5.

Аппаратно-программный комплекс для экспресс-анализа параметров импульсных помех в промышленных сетях электропитания позволяет производить определение закона распределения амплитуды импульсных

помех в сети питания, проводить экспресс-анализ параметров законов распределений амплитуды импульсных помех в сети питания и определять интенсивность импульсных помех в сети питания.

ЛИТЕРАТУРА

1. Внуков А.А. Защита информации: Учеб. пособие для бакалавриата и магистратуры - 2-е изд., испр. и доп. – М.: Юрайт, 2018. – 261 с.
2. Журнал «Информационно-управляющие системы» [Электронный ресурс] https://www.i-us.ru/jour.
3. Ключев А.О., Кустарев П.В., Платунов А.Е. Распределенные информационно-управляющие системы: Учеб. пособие. – СПб.: Университет ИТМО, 2015. - 58 с.
4. Родичев Ю. Нормативная база и стандарты в области информационной безопасности: Учеб. пособие. - СПб.: Питер, 2017. – 256 с.
5. Скабцов Н. Аудит безопасности информационных систем. – СПб.: Питер, 2018. – 272 с.
6. Шаньгин В.Ф. Информационная безопасность и защита информации. – М.: ДМК Пресс, 2018. – 702 с.
7. https://lizochekk.jimdo.com