На правах рукописи

ЧЕРЕПАНОВ Евгений Олегович

РАЗРАБОТКА И РЕАЛИЗАЦИЯ МЕТОДОВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ УПРАВЛЕНИЯ КОМПЛЕКСАМИ БЕЗОПАСНОСТИ

Специальность 05.13.01 – Системный анализ, управление и обработка информации (образование, природопользование, муниципальное управление)

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук

г. Дубна – 2004 г.

Работа выполнена в Международном университете природы, общества и человека «Дубна».

Научный руководитель:
кандидат физико-математических наук, старший научный сотрудник — СЕННЕР Александр Евгеньевич

Официальные оппоненты:

доктор технических наук, профессор — ТРОФИМОВ Александр Терентьевич

кандидат технических наук, старший научный сотрудник — ДОВГУН Валерий Афанасьевич

Ведущее научно-исследовательское учреждение: Всероссийский Научно-Исследовательский Институт Технической Физики и Автоматизации

Защита диссертации состоится 24.12 2004 года в 16 часов в аудитории 1-300 на заседании диссертационного совета К800.017.01 при Международном университете природы, общества и человека «Дубна».

С диссертацией можно ознакомиться в библиотеке Международного университета природы, общества и человека «Дубна», по адресу: Московская обл., г. Дубна, ул. Университетская, д. 19.

Автореферат разослан «23» ноября 2004 года.

Ученый секретарь диссертационного совета
кандидат физико-математических наук Токарева Н.А.

Актуальность темы.

В связи с возрастающей с каждым годом опасностью техногенных катастроф и террористических актов эффективные и надежные системы безопасности особо важных объектов становятся все более востребованными в РФ. Под особо важными объектами в данной работе подразумеваются градообразующие предприятия, атомные станции, оборонные комплексы и иные объекты, обладающие значительными площадями внутренних помещений и большими территориями, подлежащими особому контролю. Для обеспечения безопасности подобных объектов требуется применение нескольких систем различного функционального назначения — охранных, пожарных, видеонаблюдения, контроля и управления доступом и т.д. Основная задача таких систем — предотвращение противоправных действий, направленных против охраняемого объекта, и обеспечение экологической безопасности прилегающих к нему территорий.

В настоящее время наблюдается устойчивая тенденция к интеграции перечисленных систем безопасности различного назначения в единые комплексы — интегрированные комплексы безопасности. Развитие информационных технологий позволило повысить степень автоматизации систем управления комплексами безопасности и обеспечило качественно новые возможности при интеграции их подсистем. Основная нагрузка при решении задач автоматизации возлагается на разработчиков программного обеспечения систем управления комплексами безопасности.

Системы управления интегрированных комплексов безопасности обладают сложной архитектурой, состоящей из множества элементов и связей между ними. Структуру элементов можно условно разделить по функциональному назначению на три основных уровня. Нижний уровень — уровень сбора и первичной обработки информации, средний уровень — хранения и структурирования данных по определенной подсистеме комплекса, верхний — обработки и представления информации по всем подсистемам комплекса. Основная часть элементов, образующих перечисленные уровни — это различные программно-аппаратные средства сбора и обработки информации, представляющие собой значительные объемы сложного дорогостоящего оборудования. Окончательное формирование и монтаж всех трех уровней производится непосредственно на объекте контроля, но к этому моменту должны быть уже завершены разработка, отладка и испытания программного обеспечения системы управления комплексом безопасности. Ввиду невозможности использования большей части элементов реального оборудования для отладки и тестирования программного обеспечения, возникает задача разработки комплекса имитационных систем, позволяющих моделировать сигналы реальных программно-аппаратных средств сбора и обработки информации, генерировать события и адекватно реагировать на управляющие воздействия.

Проведенный в рамках диссертационной работы анализ программных продуктов, производимых ведущими разработчиками комплексов безопасности в РФ, выявил отсутствие в их составе единых средств имитационного моделирования систем безопасности. Наиболее ощутимо потребность в использовании единых имитационных систем ощущается на этапе комплексных испытаний оборудования систем безопасности и при обучении обслуживающего персонала. Это обусловило необходимость разработки собственного единого комплекса имитационных систем.

Разработка отдельных специализированных имитационных систем для каждого типа и класса оборудования целесообразна только на первоначальном этапе тестирования и отладки функциональных модулей комплекса безопасности. Однако при окончательной сборке и монтаже всех подсистем комплекса, возникают задачи полномасштабной имитации оборудования для проведения испытаний системы в целом и для обучения обслуживающего персонала комплекса безопасности. Для этих целей необходимо построить единую модель программно-аппаратных средств комплекса безопасности, выделить общие для всех типов оборудования элементы и определить их основные связи и функциональные особенности. На основе построенной модели провести интеграцию имитационных средств оборудования различного функционального назначения в единый имитационный комплекс и обеспечить его универсальность и возможность расширения. Решение данной задачи позволит повысить эффективность применения имитационных средств на окончательном этапе сборки, монтажа и пуско-наладки комплекса безопасности и откроет ряд ранее недоступных возможностей по использованию имитационных систем в целях обучения и контроля качества работы обслуживающего персонала в период эксплуатации комплекса.

Цель диссертационной работы

Целью исследований является разработка и реализация методов имитации оборудования различного функционального назначения, обеспечивающих повышение качества и эффективности тестирования, испытаний и эксплуатации систем управления комплексом безопасности.

В соответствии с целью исследования в работе поставлены следующие задачи:

- провести системный анализ программно-аппаратной архитектуры комплекса безопасности, выделить основные ее элементы, их связи и отношения и, на основе результатов анализа, построить унифицированную модель программно-аппаратной архитектуры комплекса безопасности;
- разработать критерии отбора элементов программно-аппаратной архитектуры комплекса безопасности, требующих имитационного моделирования и выделить множество элементов, подлежащих имитации;
- на основе построенной модели программно-аппаратной архитектуры комплекса безопасности разработать единый интегрированный комплекс имитационных систем, состоящий из унифицированных модулей имитации оборудования различного функционального назначения.

Методы исследований

В основе исследований, выполненных в диссертационной работе, лежат системный подход и методы системного анализа с использованием элементов теории управления, системного моделирования и методик проведения испытаний программного обеспечения.

Научная новизна

Научная новизна диссертационной работы заключается в следующем:

- предложена универсальная масштабируемая модель программно-аппаратных средств контроля систем безопасности, отличающаяся интеграцией систем имитации охранного оборудования различного функционального назначения;
- предложены методы проведения комплексных испытаний систем безопасности в условиях предельных загрузок каналов данных, основанные на разработанных алгоритмах генерации событий, обеспечившие повышение достоверности оценки надежности испытываемых систем;
- разработаны и впервые в данной области применены методы обучения и контроля качества работы персонала комплекса безопасности в условиях реального объекта на основе динамической замены физических каналов данных имитационными без применения аппаратной перекоммутации.

Практическая значимость

Практическая значимость разработки определяется следующими положениями:

- применение созданных имитационных модулей обеспечило возможность параллельной разработки элементов системы и их автономного тестирования до окончательной сборки комплекса безопасности, что сократило общую длительность этапа разработки программного обеспечения;
- интеграция модулей имитации подсистем комплекса различного функционального назначения позволила сократить объемы оборудования, предназначенного для взаимодействия оператора и систем имитации на этапе окончательной сборки и эксплуатации комплекса безопасности;
- разработанные методы проведения обучения и обеспечения контроля качества работы персонала, примененные в комплексах безопасности особо важных объектов, могут использоваться в аналогичных целях на объектах иного значения.

Апробация работы

Положения и результаты диссертационной работы были доложены на семинарах кафедры системного анализа и управления Международного университета «Дубна» и на конференциях, проводимых университетом «Дубна», УНЦ ОИЯИ и РАО ЕЭС.

Результаты проведенных исследований и созданные методики опробованы и успешно применяются при разработке программного обеспечения управления системами безопасности, производимыми ОАО «Приборный завод Тензор» в городе Дубна.

Разработанное программное обеспечение установлено и функционирует в составе систем контроля комплексов безопасности более 30-ти особо важных объектов. При этом решаются задачи как обеспечения собственной безопасности объектов, так и прилегающих к ним территорий.

Методики имитации событий положительным образом зарекомендовали себя при обучении обслуживающего персонала комплексов безопасности и активно используются в учебно-испытательных целях.

Структура и объем диссертации

Диссертация состоит из введения, четырех глав, заключения общим объемом 102 страницы и списка литературы, включающего 30 наименований.

Личный вклад

По результатам выполненных исследований опубликовано 8 печатных работ, которые полностью отражают содержание диссертации, из них 7 работ опубликовано в соавторстве (перечень публикаций на последней странице автореферата).

Автором диссертации выполнено построение универсальной масштабируемой модели программно-аппаратных средств комплекса безопасности, разработка на ее основе модулей имитации сигналов оборудования и методов их применения на архитектурных уровнях аппаратной структуры комплекса. Произведена интеграция модулей имитации устройств различного функционального назначения в единый имитационный комплекс, в рамках которого реализованы разработанные алгоритмы генерации событий. Разработаны методы обучения и контроля качества работы персонала систем безопасности на основе единого имитационного комплекса. При непосредственном участии автора проводилась реализация и внедрение разработанных методов и программных средств в ряде крупных проектов.

Краткое описание диссертации

Во введении обосновывается актуальность производимых автором исследований. Рассматриваются проблемы обеспечения безопасности особо важных объектов и экологического контроля прилегающих к ним территорий. Обосновывается необходимость интеграции подсистем различного назначения в современных комплексах безопасности. Рассматривается архитектура аппаратно-программных средств комплекса безопасности. Особо подчеркивается потребность разработчиков программного обеспечения и заказчиков в многофункциональных системах имитации оборудования систем безопасности, позволяющих повысить эффективность как отладки и тестирования программного обеспечения, так и процесса обучения и контроля обслуживающего персонала.

В первой главе диссертации производится постановка решаемой задачи — формулируются проблемы, определяются основные цели исследований и устанавливаются требования, предъявляемые к результату.

Проводится сравнительный анализ специализированных программных продуктов трех производителей охранных систем, широко известных в сфере обеспечения безопасности особо важных объектов. Даны характеристики основных технических средств, используемых при обеспечении безопасности особо важных объектов. В частности, рассматриваются методики контроля и управления, реализуемые в комплексах

безопасности ОАО Тензор, описаны аппаратные и программные решения задач сбора и обработки информации. Затем описывается архитектура комплекса безопасности особо важного объекта на примере программно-аппаратных средств, производимых ОАО Тензор, и выделяются основные уровни транспортировки и обработки данных.

В заключение рассматриваются проблемы имитации событий в системах безопасности, определяются основные задачи и функции имитационных систем, описываются особенности их применения и производится их классификация.

В результате проведенного анализа предметной области и особенностей поставленных задач выявлены и сформулированы следующие проблемы:

- длительность этапов отладки программного обеспечения и невозможность автономного тестирования отдельных модулей до окончательной сборки;
- отсутствие единой структуры данных протоколов обмена с оборудованием различного функционального назначения;
- необходимость проведения обучения обслуживающего персонала в реальных условиях работы в виду отсутствия специализированных имитационных тренажеров.

В связи с предъявленными требованиями, разрабатываемые методы и программные средства должны обеспечивать:

- моделирование реальных информационных каналов, точно соответствующее протоколам имитируемого оборудования;
- генерацию и передачу по каналам связи множества возможных состояний имитируемого оборудования;
- адекватную реакцию на управляющие воздействия;
- возможность размещения на всех уровнях программно-аппаратной архитектуры комплекса безопасности;
- наличие пользовательского интерфейса для настройки параметров имитации и ручной генерации событий;
- автоматическую генерацию событий в соответствии заданным алгоритмам;
- возможность динамической замены реальных каналов данных имитационными без применения аппаратной перекоммутации.

Архитектура оборудования комплекса безопасности

Архитектуру системы контроля программно-аппаратных элементов комплекса безопасности можно условно разделить на три основных уровня, отличающихся функциональным назначением.

Нижний уровень архитектуры системы контроля состоит из аппаратных средств сбора и первичной обработки информации — различных датчиков (пожарных, охранных и т.д.) и периферийных контроллеров.

К среднему уровню архитектуры относятся программно-аппаратные средства обработки и хранения информации, получаемой с нижнего уровня, способные автономно функционировать и обладающие примитивными терминалами взаимодействия с оператором. При этом устройства среднего уровня обеспечивают передачу данных верхнему уровню и способны воспринимать управляющие воздействия в зависимости от режима функционирования.

Верхний уровень представляет собой, как правило, вычислительные системы с соответствующим программным обеспечением, предназначенным для взаимодействия одного или нескольких операторов с элементами комплекса безопасности.

При распределенной архитектуре органов управления системами комплекса безопасности, верхний уровень разделяется на два подуровня — серверный и клиентский.

Серверный уровень аккумулирует в себе информацию по всем подсистемам комплекса безопасности, обеспечивает ее передачу клиентам и транслирует на средний уровень полученные от них управляющие воздействия.

Элементы клиентского уровня обеспечивают непосредственное отображение оператору состояний и событий определенной подсистемы комплекса или всего объекта в целом, в зависимости от назначения рабочего места.

Обзор и анализ существующих систем

Из существующих на рынке РФ систем безопасности проанализированы продукты трех известных компаний, работающих в сфере обеспечения физической защиты особо важных объектов:

- Алгонт (г. Калуга)
- Альфа-Прибор (г. Тула)
- Безопасность (г. Москва)

По своим функциональным возможностям продукты всех перечисленных компаний сопоставимы и это вполне естественно, поскольку для применения на особо важных объектах они обязаны удовлетворять общим требованиям. Но есть масса отличий в методике отображения информации, конфигурирования систем, а так же в обслуживании.

Компания «Алгонт» избрала в качестве СУБД систему ORACLE, которая требует непрерывного квалифицированного обслуживания и администрирования, что зачастую невозможно ввиду отсутствия соответствующих специалистов на охраняемом объекте.

Компания «Альфа-прибор» за основу всего комплекса безопасности взяла системы видеонаблюдения, и нельзя не отметить высокую эффективность и качество данных систем. Но, тем не менее, очень мало уделено внимания графическим планам объектов и отображению их состояний, а также отсутствует возможность обобщения состояний нескольких объектов

Пользовательский интерфейс системы компании «Безопасность» применяет только растровую графику для отображения контролируемого объекта, а также не

содержит активных графических объектов большой площади. Система отображения протоколированных событий не использует цветовую градацию строк и обработку приоритетов сообщений.

Модули реального времени описанных систем достаточно открыты для пользователя и не позволяют ограничить доступ как к файлам самого продукта, так и к ресурсам операционной системы. Этот факт является серьезным недостатком в условиях обеспечения безопасности особо важных объектов, где особо важно предотвратить как непроизвольное, так и преднамеренное нарушение работы систем контроля комплекса.

Ни один из рассмотренных продуктов не обладает комплексом систем имитации, необходимых для проведения испытаний и обучения персонала.

В результате проведенного анализа рассмотренных выше программных продуктов можно сделать вывод, что методики решения задач обеспечения безопасности, примененные фирмами «Алгонт», «Альфа-Прибор» и «Безопасность» обладают рядом недостатков, часть из которых весьма существенна. Это обусловило необходимость, учитывая несомненные достоинства перечисленных продуктов, разработать собственную методику построения систем контроля и управления, исключающую перечисленные недостатки рассмотренных продуктов.

Анализ и классификация имитационных систем

Проведен анализ особенностей применения имитационных средств в сфере безопасности, позволивший провести классификацию существующих имитационных систем. В результате установлено, что имитационные системы могут быть как аппаратными, так и программными. Программные системы, в свою очередь, разделяются на внутренние и внешние.

Аппаратные имитационные системы представляют собой конструктивные изделия, которые аккумулируют в себе функции прибора, предназначенного для сбора и обработки данных, а также функции датчиков как источников информации.

Основные преимущества аппаратных имитационных систем заключаются в том, что для их использования не требуется персонал с высокой квалификацией. Также аппаратные системы отличаются высокой надежностью и низкими требованиями к условиям эксплуатации.

К недостаткам аппаратных имитационных систем следует отнести ограничения по быстродействию и функциональным возможностям, а также высокую стоимость и длительность изготовления.

Программные имитационные системы представляют собой приложения или библиотеки, установленные на компьютере, позволяющие генерировать поток данных по физическим (внешние системы) или виртуальным (внутренние системы) информационным каналам.

Основное преимущество программных имитационных систем связано с компактностью и простотой в эксплуатации. При этом настройки параметров функционирования виртуального оборудования достаточно гибкие для имитации различных нештатных ситуаций и аварийных режимов. В программные имитационные

системы, как правило, заложена возможность генерации случайных с событий с определенной частотой. Интенсивность этих событий может значительно превышать реальную, что позволяет тестировать программное обеспечение в гораздо более жестких режимах.

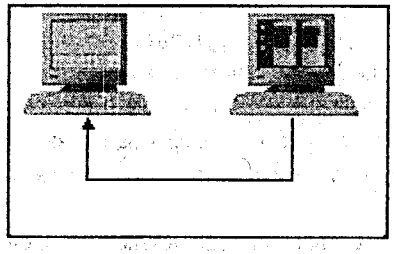
Программные имитационные системы могут размещаться на различных архитектурных уровнях передачи данных, что позволяет более эффективно проводить тестирование и испытания программного обеспечения и аппаратуры. Также программные системы отличаются значительно более низкими затратами на производство и тиражирование.

Основным недостатком программных имитационных систем является необходимость использования вычислительной техники для их применения и как следствие — ограниченные условия эксплуатации и достаточно высокая квалификация персонала.

Внешние имитационные системы представляют собой программные или аппаратные средства, предназначенные для генерации событий и реакции на управляющие воздействия по физическим каналам данных, используя реальные протоколы взаимодействия контроллеров и вычислительной техники. Взаимодействие внешних имитационных систем и программных средств контроля и управления происходит, как правило, по интерфейсам RS232, RS485, CAN или сети Ethernet.

Задачей внешних имитационных систем является адекватная замена одной или нескольких аппаратных частей комплекса без внесения каких-либо конструктивных и программных изменений в остальные части.

Основным преимуществом внешних имитационных систем является имитация аппаратной части комплекса безопасности, не оказывающая влияний на программные средства контроля и управления.



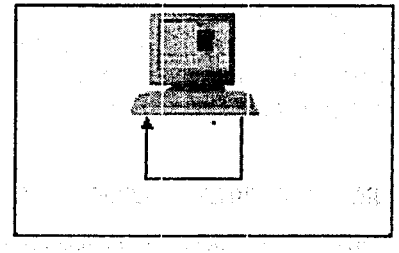
Внешняя имитационная система.

К недостаткам таких систем относится необходимость перекоммутации физических каналов для их подключения, что требует временных затрат и привлечения специалистов.

Внутренние имитационные системы представляют собой программные средства в виде приложений или библиотек, позволяющих заменить собой драйвер контроллера или модуль клиента системы распределенного контроля.

Задачей внутренних имитационных систем является моделирование функциональных свойств всей аппаратной части комплекса безопасности вместе с физическими каналами передачи данных и интерфейсными устройствами.

Основным преимуществом внутренних имитационных систем является возможность имитации аппаратной части комплекса безопасности без использования каких-либо физических линий и независимо от настроек и особенностей контроллеров. В связи с этим отпадает необходимость перекоммутации линий связи и появляется возможность динамического переключения каналов данных.



Внутренняя имитационная система.

Недостатком внутренних имитационных систем является неполная идентичность имитируемой аппаратной части и необходимость их внедрения в систему контроля.

Проведенная классификация и анализ особенностей имитационных систем различных типов позволили разработать собственную методику применения имитационных средств на этапах отладки, тестирования и испытаний программного обеспечения комплекса безопасности.

Во второй главе рассматривается построение унифицированной модели программно-аппаратной архитектуры комплекса безопасности и единой структуры данных протоколов обмена оборудования различного функционального назначения.

Далее проводится анализ и применение методов модульного и комплексного тестирования программного обеспечения.

В заключение второй главы описаны разработанные алгоритмы генерации событий, примененные для испытания программного обеспечения комплекса безопасности.

Разработка модели программно-аппаратной архитектуры комплекса безопасности

При построении модели программно-аппаратной архитектуры комплекса безопасности, описываются основные ее элементы, их функциональное назначение, отношения и связи. Затем выделяются элементы, имитационное моделирование которых необходимо для решения поставленных задач.

Применяя последовательное рассмотрение архитектуры «снизу вверх», в первую очередь описываются оконечные устройства — регистрирующие и исполнительные элементы подсистем безопасности. Прежде всего, это источники информации (средства обнаружения, датчики), обладающие собственным перечнем принимаемых состояний или значений в зависимости от типа и управляемые устройства (замки, средства пожаротушения), обладающие перечнем команд.

Следующим элементом модели является сектор — устройство определенного типа и функционального назначения (периферийный контроллер), обладающее перечнем

источников информации и управляемых устройств, способное передавать информацию о состояниях своих элементов, принимать и обрабатывать команды.

Сектора объединяются в группы устройств по принадлежности к определенному типу или физической привязке к одному контроллеру среднего уровня.

Полученные группы устройств вместе с каналами связи образуют подмножество элементов общей структурной модели комплекса безопасности, подлежащих имитации.

Предложенная модель легла в основу имитационных модулей, моделирующих функциональные свойства отдельных типов оборудования, а универсальность данной модели позволила провести интеграцию имитационных систем в единый имитационный комплекс.

Универсальная структура данных протокола обмена с оборудованием

Для обеспечения эффективного взаимодействия систем контроля и аппаратуры комплекса безопасности разработана универсальная структура данных протокола обмена с нижним уровнем, позволяющая одновременно опрашивать разнотипные устройства.

Созданная структура данных основана на принципе единообразия составных элементов оборудования. В результате формализации структурных составляющих нижнего уровня предложено следующее множество типов информационных источников: охранный шлейф, пожарный шлейф, шлейф технического контроля, шлейф контроля доступа, аналоговый шлейф, ключ управления, цифровой вход.

Не смотря на то, что каждый из этих источников обладает собственным перечнем управляющих команд, все состояния, которые он принимает, содержатся в общем множестве состояний. При установке соединения с устройством нижнего уровня, посредством универсальной структуры данных, опрашиваемое оборудование предоставляет описание своей архитектуры, передавая перечень подключенных к нему информационных источников. На основании полученной информации, верхний уровень формирует собственную структуру данных.

Алгоритмы генерации событий при испытании программного обеспечения

Основными задачами испытаний комплекса безопасности являются:

- выявление максимальной интенсивности событий, при которой все события регистрируются системами контроля;
- определение времени наработки на отказ в условиях длительных испытаний при максимальной интенсивности событий.

Для решения перечисленных задач необходимо моделирование эксплуатации систем контроля в условиях предельных загрузок каналов данных. В качестве средств моделирования сигналов оборудования используются автономные элементы разработанного комплекса имитационных систем. Каждый элемент имитирует сигналы определенного периферийного контроллера (сектора), используя разработанные алгоритмы генерации событий.

С целью проверки работоспособности программного обеспечения в разных условиях, генерация событий производится попеременно в импульсном и равномерном режимах. Импульсный режим характеризуется периодической генерацией значительного числа событий за короткий промежуток времени. При этом период возникновения импульсов на 2-3 порядка превышает длительность самих импульсов. Равномерный режим является частным случаем импульсного и характеризуется генерацией одиночных событий через равные промежутки времени, меньшие, чем период импульсного режима, но большие, чем длительность импульсов. При этом обеспечивается приблизительное равенство количества событий за длительный промежуток времени и в том, и в другом режиме.

При импульсном режиме испытаний необходимо обеспечить синхронизацию импульсов генерации событий на автономно работающих модулях имитации, а при равномерном режиме решается обратная задача — необходимо равномерно распределить начало генерации событий в пределах одного периода на всех модулях. При условии синхронизации системного времени на всех вычислительных машинах комплекса безопасности и единых параметров генерации событий для всех имитационных модулей, решение поставленных задач заключается в вычислении времени начала генерации событий для каждого имитационного модуля.

Прежде всего, необходимо описать параметры, обеспечивающие генерацию событий в заданном режиме:

T_0 — время отправки первому имитационному модулю команды начала генерации событий;

ΔT — период возникновения импульсов;

$\Delta T_{случ}$ — случайное значение в пределах от 0 до ΔT с равномерным и непрерывным распределением.

$T_{i\,получ}$ — время получения команды начала генерации i-м модулем;

$T_{i\,нач}$ — время начала генерации событий для i-го модуля;

тогда время начала генерации событий в импульсном режиме для i-го модуля вычисляется по формуле:

$$T_{i\,нач} = T_{i\,получ} + (\Delta T - \left\{ \frac{T_{i\,получ} - T_0}{\Delta T} \right\}) \bullet \Delta T,$$

где фигурные скобки означают операцию выделения дробной части числа, заключенного в скобки. В итоге, каждый имитационный модуль обеспечивает старт генерации событий через промежуток времени с момента вызова первой команды, кратный периоду генерации импульсов, что обеспечивает их синхронизацию.

Для обеспечения равномерного режима время начала генерации событий для i-го модуля вычисляется по формуле:

$$T_{i\,нач} = T_{i\,получ} + \Delta T_{случ},$$

в этом случае, при условии значительного количества имитационных модулей, распределение возникновения событий близко к равномерному.

Реализация в рамках имитационных модулей предложенных алгоритмов обеспечила проведение испытаний комплекса безопасности в условиях предельных загрузок каналов данных и в соответствии заданным режимам генерации событий.

Третья глава посвящена разработке программного обеспечения единого имитационного комплекса. В первую очередь описывается разработка систем имитации оборудования различного функционального назначения.

Далее решаются задачи интеграции имитационных систем в единый имитационный комплекс на основе описанной выше модели программно-аппаратной архитектуры комплекса безопасности.

В заключение третьей главы описаны методы и особенности распределенного размещения имитационных модулей.

Разработка систем имитации

Как уже было отмечено выше, внутренние имитационные системы представляют собой программные средства в виде приложений или библиотек, позволяющих заменить собой драйвер контроллера или модуль клиента системы распределенного контроля.

Для обеспечения внутренней имитации в системе контроля и управления комплексом безопасности разработаны соответствующие библиотеки, обладающие внутренним программным интерфейсом, идентичным драйверу реального обмена, а также внешним пользовательским интерфейсом для взаимодействия с оператором.

Внешний пользовательский интерфейс внутренних имитационных систем формируется в соответствии с особенностями моделируемого устройства, при этом обеспечивается единообразие с имитационными средствами других устройств. Поскольку предполагается, что оператор будет обслуживать несколько разнотипных подсистем комплекса, имитационные системы также отличаются между собой по типу имитируемых устройств. Не смотря на это, оператор не должен испытывать затруднений при переключении между различными средствами имитации.

Основной задачей внутренних имитационных систем является моделирование функциональных свойств аппаратных средств комплекса безопасности вместе с физическими каналами передачи данных и интерфейсными устройствами. Поэтому, помимо имитации событий, происходящих на объекте, внутренние имитационные системы позволяют имитировать состояния каналов связи, включая генерацию помех и ошибочных обменов.

Внешние имитационные системы представляют собой программные или аппаратные средства, предназначенные для генерации событий и реакции на управляющие воздействия по физическим каналам данных, используя реальные протоколы взаимодействия контроллеров и вычислительной техники.

Внутренний интерфейс обмена внешних имитационных систем полностью соответствует протоколу взаимодействия верхнего и среднего уровней. Подключение внешней имитационной системы не отражается на работе программного обеспечения верхнего уровня.

С целью обеспечения единообразия пользовательский интерфейс внешних систем приближен к интерфейсу соответствующих внутренних средств имитации.

Распределенное размещение имитационного комплекса

Выше были описаны особенности внешнего и внутреннего размещения имитационных средств и их применение на этапах разработки и отладки программного обеспечения. Однако, для итоговых испытаний комплекса безопасности и проведения обучения непосредственно на объекте контроля наиболее предпочтительным является распределенное размещение имитационной системы, при котором программные модули имитации расположены на серверном уровне, а их настройка и управление осуществляется непосредственно с клиентских мест. При этом обеспечено динамическое переключение между дежурным и имитационным режимами без аппаратной перекоммутации. Таким образом, любое из клиентских мест может дистанционно переключаться в имитационный режим с определенного рабочего места, например, оператора, проводящего курс обучения или проверки квалификации персонала, при этом обучаемые операторы на своих рабочих местах будут находиться вне ведома о том, получают ли они реальную информацию или имитационную. Этот подход позволил более эффективно и безопасно проводить обучение персонала и осуществлять контроль качества его работы в дежурном режиме.

В четвертой главе содержатся описания методик испытаний и экспериментов и результаты, полученные на этапе внедрения разработанного программного обеспечения.

В первую очередь рассматривается методика стендовых испытаний программного обеспечения системы контроля комплекса безопасности с применением имитационных пакетов, затем проводятся испытания на реальном оборудовании.

Далее приводятся результаты испытаний, проведенных непосредственно на объектах с участием обслуживающего персонала и описываются методы обучения операторов.

В заключение рассматриваются перспективы дальнейшего развития и применения разработанных методик.

Стендовые испытания с применением имитационных систем

Перед вводом в эксплуатацию программного обеспечения комплекса безопасности проводится ряд испытаний с тем, чтобы установить основные показатели качества работы системы. Для определения отказоустойчивости и безошибочности функционирования программного обеспечения и каналов связи необходимы длительные испытания. Однако длительность можно сократить за счет искусственного ужесточения условий испытания, используя описанные выше алгоритмы генерации событий. До разработки комплекса программных имитаторов это было не возможно. Имея же, описанные выше имитационные системы, стендовые испытания с их применением становятся значительно более эффективными, при этом значительно сокращается время, затрачиваемое на этом этапе испытаний.

Испытания СКУ на реальном оборудовании

При подключении программного обеспечения комплекса безопасности к реальному оборудованию оценивается в основном качество и эффективность работы аппаратных средств и коммуникационных каналов. Проводятся испытания на общую скорость реакции системы, проверяется работа систем в аварийных режимах — при обрыве части информационных каналов или при переходе на резервное питание.

Все эти эксперименты также требуют применения имитационных систем, причем, обладающих способностью дистанционного переключения каналов данных без аппаратной перекоммутации. Это необходимо для обеспечения возможности параллельного анализа работы программного обеспечения с имитационными системами и с реальным оборудованием, а также для оперативного выделения неисправностей в случае их возникновения.

Результаты экспериментов, проведенных на объектах

При проведении экспериментов на объектах в основном оценивались характерные времена, затрачиваемые персоналом на те или иные действия с программным средствами имитации (ПСИ). Затем эти времена сравнивались с аналогичными значениями, полученными при работе с аппаратными средствами генерации событий — стендами проверки приборов (СПП) серии «Кристалл 2С» (эксперимент проводился с использованием 24-х СПП, расположенных в одном помещении).

Время, необходимое оператору на указанное действие (с.)

Действие	ПСИ	СПП
Генерация определенного события на одном секторе	1	1
Генерация определенного события на 10 определенных секторах	5	26
Генерация определенного события на всех (24) секторах	3	38
Сброс всех тревожных значений на одном секторе	1	12
Сброс всех тревожных значений на 10 определенных секторах	5	94
Сброс всех тревожных значений на всех (24) секторах	3	142
Запуск автоматической генерации событий на одном секторе	2	нет

Результаты эксперимента показали, что при увеличении объемов имитируемого оборудования, растет эффективность применения программных средств имитации для генерации событий в комплексах безопасности.

Обучение и контроль действий персонала

Основная задача при обучении персонала заключается в оперативной передаче навыков в работе с системой и обеспечение дальнейшей ее работы без привлечения разработчиков. Процесс обучения может вестись различными методами, но как показал опыт — наиболее эффективны практические тренировки. Зачастую обучение приходится проводить непосредственно во время установки систем безопасности на объекте, используя при этом сигналы с реальных датчиков и систем контроля, находящихся на боевом дежурстве. Для избежания этого, а также для повышения эффективности обучения, применяются разработанные системы имитации с принципом горячего переключения, управляемые с отдельного клиентского рабочего места.

Помимо повышения безопасности работы всех систем на объекте во время обучения, возникла возможность проводить оценку действий персонала с системами комплекса в режимах псевдо тревог и при моделировании внештатных ситуаций. В результате применения описанных выше методов, время обучения удалось сократить в 1,5 раза без снижения качественных показателей, при этом появились качественно новые, недоступные ранее, средства контроля исполнения обязанностей персонала во время дежурства.

В заключение указаны основные результаты, достигнутые в диссертационной работе.

Проведен анализ программно-аппаратной архитектуры комплекса безопасности и предложены критерии отбора элементов системы, требующих имитационного моделирования. Построена универсальная масштабируемая модель программно-аппаратной архитектуры комплекса безопасности, обеспечившая интеграцию систем имитации охранного оборудования различного функционального назначения.

Разработан единый интегрированный комплекс имитационных систем, в рамках которого реализованы алгоритмы генерации событий, обеспечившие проведение испытаний контролирующего оборудования и программного обеспечения в условиях предельных загрузок каналов данных, что дало возможность определить запас устойчивости и производительность системы контроля и управления комплексом безопасности.

Разработан метод дистанционной замены реальных каналов данных имитационными без аппаратной перекоммутации, обеспечивший качественно новые возможности проверки квалификации и контроля работы обслуживающего персонала комплекса безопасности.

На 40-50% ускорены процессы пуско-наладки программных модулей за счет обеспеченных разработанными имитационными средствами возможностей параллельной разработки элементов системы и их автономного тестирования до окончательной сборки комплекса безопасности.

В 1,5 раза сокращено время обучения персонала комплекса безопасности и обеспечена безопасность проведения образовательного процесса в результате применения разработанного единого имитационного комплекса.

Список работ, опубликованных по теме диссертации

[1] Черепанов Е.О. Методика организации представления информации в системах управления комплексом безопасности // Сборник научных трудов кафедры САУ. Вып. 1. – Дубна: Международный университет природы, общества и человека «Дубна», 2002. – – с. 186-200.

[2] Черепанов Е.О., Скачков Н.Б. Программный комплекс представления и обработки экспериментальных данных // Сообщение ОИЯИ. — Дубна 2002 г., Р10-2002-279

[3] Черепанов Е.О., Журавлев П.П. Методика контроля состояний комплекса безопасности и универсальный интерфейс передачи данных к элементам отображения // Сборник докладов IX Междисциплинарной студенческой научной конференции университета Дубна. — Дубна, 2003 г. — с.358-363.

[4] Черепанов Е.О., Скачков Н.Б. Программный пакет представления и обработки экспериментальных данных // Сборник докладов VII конференции ОМУС ОИЯИ. — Дубна: ОИЯИ, 2003 г., с. — 322-326.

[5] Черепанов Е.О., Журавлев П.П. Методика контроля состояний комплекса безопасности и универсальный интерфейс передачи данных к элементам отображения // Сборник докладов I ежегодной научной конференции студентов университета «Дубна» и УНЦ ОИЯИ. - Дубна: ОИЯИ, 2003 г.— с.246-250.

[6] Черепанов Е.О., Журавлев П.П. Имитация событий в системах реального времени и ее использование в учебно-испытательных целях // Сборник докладов VIII конференции ОМУС ОИЯИ. – Дубна: ОИЯИ, 2004 г. — с.304-308.

[7] Журавлев П.П., Черепанов Е.О. Программное обеспечение верхнего уровня системы охранной сигнализации СОС-1 // Сборник докладов конференции «Системы физической защиты особо важных объектов РАО ЕЭС». — Дубна: Тензор, 2004 г.

[8] Черепанов Е.О., Журавлев П.П. Имитация событий в системах безопасности и ее использование в учебных и испытательных целях // Сборник докладов X междисциплинарной студенческой научной конференции университета Дубна. — Дубна: Международный университет природы, общества и человека «Дубна», 2004 г.— с.321-325.