ЗАО "НПЦ ИРС" НИУ "МИЭТ" ООО "ИНТЕХ"

ВСЕРОССИЙСКАЯ МЕЖВЕДОМСТВЕННАЯ НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

МОСКВА 20.10.2020

НАУКА И АСУ 2020

по теоретическим и прикладным проблемам развития и совершенствования АСУ и связи специального назначения

СБОРОНИК ТЕЗИСОВ

Закрытое акционерное общество
«Научно-производственный центр
информационных региональных систем»
(ЗАО «НПЦ ИРС»)

Национальный исследовательский университет «Московский институт электронной техники»
(НИУ «МИЭТ»)

Общество с ограниченной ответственностью
«Институт инноваций и наукоемких технологий»
(ООО «Институт «ИНТЕХ»)

СБОРНИК ТЕЗИСОВ

ВСЕРОССИЙСКОЙ МЕЖВЕДОМСТВЕННОЙ НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ

по теоретическим и прикладным проблемам развития и совершенствования автоматизированных систем управления и связи специального назначения «НАУКА И АСУ — 2020»

20 октября
Москва, Зеленоград

Всероссийская межведомственная научно-техническая конференция по теоретическим и прикладным проблемам развития и совершенствования автоматизированных систем управления и связи специального назначения «НАУКА и АСУ–2020» (Москва, Зеленоград, 20 октября 2020 г.): сборник тезисов. – М. : Изд-во НИУ «МИЭТ», 2020. – 130 с.

В сборник вошли тезисы по материалам докладов участников Всероссийской межведомственной научно-технической конференции по теоретическим и прикладным проблемам развития и совершенствования автоматизированных систем управления и связи специального назначения «НАУКА и АСУ–2020».

Материалы публикуются в авторской редакции.

СОДЕРЖАНИЕ

СЕКЦИЯ № 1: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СОВРЕМЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

СЕКЦИЯ № 2: МАТЕМАТИЧЕСКОЕ, ПРОГРАММНОЕ И ИНФОРМАЦИОННО-ЛИНГВИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

СЕКЦИЯ № 1

СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СОВРЕМЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

АВТОМАТИЗИРОВАННОЕ УСТРОЙСТВО ХРАНЕНИЯ И ЭКСТРЕННОГО УНИЧТОЖЕНИЯ НОСИТЕЛЕЙ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ

Новожилов Артем Сергеевич

младший научный сотрудник, научно-исследовательский центр
Краснодарского высшего военного училища имени генерала армии С.М. Штеменко,
г. Краснодар, Россия, novozhilov-artem@bk.ru

Волкова Альбина Александровна

старший научный сотрудник, научно-исследовательский центр
Краснодарского высшего военного имени генерала армии С.М. Штеменко,
г. Краснодар, Россия, valbina@inbox.ru

На сегодняшний день в Вооруженных Силах Российской Федерации экстренное уничтожение носителей сведений, составляющих государственную тайну, осуществляется средствами, не обеспечивающими возможность уничтожения полного объёма носителей информации за короткое время. Дополнительно, процесс экстренного уничтожения, в большинстве от человеческого фактора (уничтожение производится случаев, зависит военнослужащими).

Указанные проблемы, в совокупности с, как правило, большими объёмами носителей сведений, составляющих государственную тайну, находящимися в воинских частях, увеличивают вероятность компрометации носителей информации в случаях возникновения кризисных ситуаций (стихийных бедствий, нападении противника и т.д.).

В армиях таких государств, как России, США, Китая, Франции, Германии, Японии, странах СНГ применяются следующие методы экстренного уничтожения носителей секретной информации: механический; термический; химический; физический; и метод затопления.

Средства экстренного уничтожения секретной информации в армиях различных стран отличаются по своим техническим решениям и конструкциям, однако у всех устройств и способов имеются основной недостаток – они не эффективны по отношению к современным условиям ведения военных конфликтов.

Во-первых, за счет малого количества отведенного времени на процесс уничтожения – каждый из приведённых средств экстренного уничтожения обладает малой производительностью.

Во-вторых, по технической обеспеченности войск средствами для экстренного уничтожения носителей информации, отвечающих требованиям безопасности, надежности и работоспособности.

В-третьих, по физическим возможностям личного состава произвести процесс уничтожения качественно — т.е. процесс экстренного уничтожения НССГТ зависит от человеческого фактора.

Исходя из вышесказанного, целью исследования является разработка автоматизированного устройства хранения и экстренного уничтожения носителей сведений, составляющих государственную тайну, отвечающее следующим требованиям. Хранение носителей информации в хранилище с возможностью их гарантированного экстренного уничтожения при угрозе компрометации. Быстрая скорость экстренного уничтожения носителей информации. Устройство должно обладать автоматизированным запуском средства экстренного уничтожения. Устройство должно обладать высокой надежностью, безопасностью применения и простотой обслуживания.

Модель устройства представляет собой металлический сейф, внутри которого размещены функциональные блоки.

Устройство реализует защиту от угрозы несанкционированного вскрытия спецхранилища — посредством датчика контроля целостности оболочки спецхранилища.

Внутри спецхранилища располагается блок анализа – компьютер который обрабатывает данные от технических средств и «оценивает» наличие угрозы; в его алгоритме работы предусмотрена защита от ложного срабатывания средства уничтожения (при ложных угрозах), а также автоматический его запуск при реальной угрозе (когда есть угроза несанкционированного вскрытия спецхранилища).

У спецхранилища имеется два варианта использования.

В качестве сейфа, оборудованного защитой от взлома, когда активируется режим работы хранилища, включающий защиту от взлома и далее - работает автоматически.

В качестве обыкновенного сейфа с возможностью уничтожения содержимого, когда режим работы хранилища по защите от взлома отключен, и который можно активировать в любой момент времени.

Областью применения разрабатываемого автоматизированного устройства хранения и экстренного уничтожения носителей информации могут быть подразделения секретного делопроизводства и службы защиты государственной тайны всех видов войск Вооруженных Сил Российской Федерации, Федеральная служба охраны, Федеральная служба безопасности, службы безопасности банков и частных фирм.

Ключевые слова: сейф; компрометация; автоматизированное устройство; экстренное уничтожение; государственная тайна.

АЛГОРИТМ ТРАЕКТОРНОЙ ОБРАБОТКИ ИНФОРМАЦИИ РАДИОЛОКАЦИОННЫХ ИЗМЕРИТЕЛЬНЫХ КОМПЛЕКСОВ НА ОСНОВЕ КЛАСТЕРИЗАЦИИ МЕТОДОМ K-MEANS

Кондыбаев Нурлан Сакенович
акционерное общество «Кронштадт технологии»,
г. Санкт-Петербург, Россия, nurkon@yandex.ru

Куприянов Николай Александрович
Военно-космическая академия имени А.Ф. Можайского,
г. Санкт-Петербург, Россия, sektor-ussr@rambler.ru

Куракин Сергей Зосимович
кандидат технических наук, доцент,
Военно-космическая академия имени А.Ф. Можайского,
г. Санкт-Петербург, Россия, kurakin@smtp.ru

В настоящее время наблюдаются интенсивные процессы техногенного засорения околоземного космического пространства вследствие увеличения числа космических объектов. Деятельность человеческой цивилизации по освоению космоса привела к тому, что в околоземном космическом пространстве помимо действующих космических аппаратов также находятся прекратившие работу спутники, разгонные блоки и элементы космического мусора. Это ведёт как к повышенному риску столкновений космических объектов, так и к ограничениям на использование орбитального ресурса в интересах систем локации, навигации, дистанционного зондирования земной поверхности, телевидения и связи. С учётом прогнозируемого многократного увеличения количества космических объектов в околоземном космическом пространстве и уменьшения их размера актуальной научно-технической задачей является решение вопроса повышения точности определения средствами наблюдения местоположения космических объектов.

Координатная информация о местоположении значительного количества космических объектов, расположенных на низких и средних околоземных орбитах, рассчитывается с применением различных радиолокационных измерительных комплексов, определяющих мгновенное положение наблюдаемых целей и рассчитывающих траектории их движения. Точность измерения местоположения наблюдаемых целей зависит от ряда факторов, определяемых характеристиками радиолокационного измерительного комплекса и условиями функционирования, к которым, в том числе, относятся гелиогеофизические. Применение в современных радиолокационных комплексах высокотехнологичной аппаратуры генерирования, формирования и обработки сигналов позволяет значительно снизить негативный вклад собственной шумовой составляющей в точность измерения местоположения космических объектов. Кроме того, в состав большинства современных радиолокационных измерительных комплексов включаются специальные системы учёта влияния среды распространения радиоволн, позволяющие определять гелиогеофизические условия функционирования и учитывать их влияние при определении местоположения космических объектов. Такое решение позволяет снизить негативное влияние среды распространения радиоволн на точностные характеристик радиолокационных измерительных комплексов и повысить их информационные возможности.

Опыт эксплуатации радиолокационных измерительных комплексов показал, что модели, заложенные в системы учёта влияния среды распространения, основаны на долгосрочном прогнозировании гелиогеофизических условий функционирования. При этом результаты оперативного мониторинга среды распространения радиоволн используются для адаптации программно реализованных моделей в локальных областях, а для остальных областей пространства используются интерполяционные методы и усреднённые значения параметров среды распространения радиоволн. Это ведёт к тому, что погрешности измерений местоположения космических объектов в зоне обзора радиолокационных измерительных комплексов компенсируются с низким пространственным и временным разрешением. На практике это проявляется в том, что спорадические изменения гелиогеофизических условий функционирования не учитываются при определении местоположения объектов наблюдения, что ведёт к росту ошибок измерений и снижению информационных возможностей радиолокационных измерительных комплексов.

В то же время, изменение гелиогеофизических условий функционирования может носить локальный характер, что особенно характерно для радиолокационных измерительных комплексов, имеющих широкие угловые размеры зон обзора. Определение областей пространства, в которых влияние гелиогеофизических условий функционирования увеличивает погрешности измерений, позволит компенсировать такие погрешности, что приведёт к повышению информационных возможностей радиолокационных измерительных комплексов.

В рамках представленной статьи рассмотрена идея использования невязки измерений местоположения кластеров космических объектов, по которым имеется априорная координатная информация. Представлены результаты компьютерного моделирования и показано, что предложенный подход позволяет определять области, в которых влияние гелиогеофизических условий функционирования увеличивает погрешности измерений. Изложены основные расчётные соотношения и показаны этапы алгоритма, а также предложены дальнейшие направления использования результатов его работы для повышения информационных возможностей радиолокационных измерительных комплексов.

Ключевые слова: радиолокационный измерительный комплекс, космический объект; кластерный анализ; невязка измерений.

АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ ОБЕСПЕЧЕНИЯ СОВМЕСТИМОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБЪЕДИНЕННЫХ ВООРУЖЕННЫХ СИЛ СТРАН НАТО

Кузвесов Анатолий Иванович

*кандидат технических наук, старший научный сотрудник,
27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации, г. Москва, Россия*

Пихтелев Александр Петрович

*27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,,
г. Москва, Россия, shanetambov@inbox.ru*

Бабин Степан Владимирович

*27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, stepanvb@yandex.ru*

Последовательное внедрение автоматизированных систем в России привело к тому, что они стали неотъемлемой частью процесса управления. Однако с развитием информационных (компьютерных) технологий растут и требования к автоматизированным системам, что влечет за собой непрерывный процесс их модернизации и, при достижении предела технических возможностей какой-либо системы, создание новой, отвечающей современным требованиям к ней.

Несмотря на то, что процессы создания автоматизированных систем в настоящий момент регламентированы, поддержание высокого уровня совместимости между ними по мере роста их сложности является актуальной проблемой, и существующие стандарты не позволяют решить ее в полной мере. Увеличение сложности систем приводит к тому, что основное внимание уделяется межкомпонентному взаимодействию и прямому функциональному назначению в ущерб взаимодействию с внешними системами. Разработчики систем в процессе их создания решают частные инженерные задачи для обеспечения работы функций целевой системы, упуская из виду системное окружение. В результате такой работы создаются уникальные модули (программные библиотеки, программные компоненты, структуры баз данных), в том числе интерфейсы (протоколы) взаимодействия. При этом каждый уникальный модуль подходит только конкретной системе и не подходит для использования другими разработчиками, что влечет за собой вынужденную модернизацию других систем, которым нужна функциональность такого модуля. Модернизация сложных систем по объему работ не многим отличается от создания новой, и фактически завершает этап эксплуатации исходной системы раньше отведенного времени.

Из вышесказанного следует, что повышение качества взаимодействия автоматизированных систем может существенно продлить период их эксплуатации, предоставляя разработчикам возможность вывести качество автоматизированных систем на принципиально новый уровень. На данный момент в Вооруженных Силах Российской Федерации выполнение требований по взаимодействию автоматизированных систем достигается в рамках конкретного заданного перечня, и рациональным решением повышения совместимости с другими системами (изначально

не предусмотренными) является стандартизация интерфейсов взаимодействия. Такая практика уже более 30 лет применяется при разработке автоматизированных систем в США и странах блока НАТО.

Исходя из того, что разработка универсального стандарта для обеспечения взаимодействия большинства автоматизированных систем – сложная задача, командование вооруженных сил США приняло решение о стандартизации функциональных областей информационного взаимодействия автоматизированных систем. Такое решение позволяет обновлять базу интерфейсных стандартов без нарушения общей целостности информационного пространства.

Впервые такая практика была применена в виде Руководства по практическому применению рекомендованных стандартов в области моделирования и имитации, которое является результатом трехлетней работы Modelling and Simulation Coordination Office. Позже, учитывая полученный опыт, в странах-участницах блока НАТО также были созданы рабочие группы – Modelling and Simulation Group и Modelling and Simulation Standards Subgroup. Задачей групп является создание и совершенствование профиля стандартов в области моделирования и имитации.

Руководство по практическому применению рекомендованных стандартов и профиль стандартов существенно ограничили разработчиков автоматизированных систем, однако, несмотря на ограничения, создаваемые системы смогли взаимодействовать между собой без дополнительных доработок и явных требований по совместимости. Это позволило повысить информационное взаимодействие автоматизированных систем, что, в свою очередь, повысило интенсивность проведения мероприятий подготовки вооруженных сил с использованием средств автоматизации и их качество.

В настоящее время в различных отраслях промышленности Российской Федерации существует значительное количество государственных и международных стандартов, комплексное применение которых позволяет создать основу для создания рекомендаций по стандартизации взаимодействия между автоматизированными системами (по аналогии с Руководством и Перечнем в США и странах НАТО). Однако имеется ряд объективных и субъективных причин, по которым эти рекомендации до сих пор не созданы. Из результатов анализа опыта ведущих зарубежных стран видно, что основной причиной является отсутствие органа, подобного Modelling and Simulation Coordination Office, и целенаправленного управления процессом повышения взаимодействия автоматизированных систем.

Ключевые слова: автоматизация; информационное взаимодействие; моделирование; сложность; стандартизация; совместимость.

ИЗМЕНЕНИЕ СТРУКТУРЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ОРГАНИЗАЦИЕЙ ВОЗДУШНОГО ДВИЖЕНИЯ В АЭРОПОРТУ

Убанкин Евгений Иванович

кандидат технических наук, доцент,
Дальневосточный федеральный университет,
г. Владивосток, Россия, uei@inbox.ru

Павликов Сергей Николаевич

кандидат технических наук, профессор,
Владивостокский государственный университет экономики и сервиса,
г.Владивосток, Россия, psn1953@mail.ru

Черновол Михаил Юрьевич

Владивостокский государственный университет экономики и сервиса,
г.Владивосток, Россия, kittihokk@mail.ru

Зимарёва Евгения Андреевна

Морской государственный университет имени адм. Г.И. Невельского,
г. Владивосток, Россия, fogetmenots@mail.ru

В настоящее время в развитии авиации отмечена тенденция повышения безопасности воздушных судов при необходимости увеличения эффективности за счет роста интенсивности работы взлетно-посадочной полосы аэропортов. Интенсивность, непредсказуемость условий внешней среды и эксплуатации судов, а также увеличение их размеров способствует снижению безопасности. Посадка в первую очередь является рискованным этапом полета. Отмечается рост число аварий по причине отсутствия автоматизированной системы управления с возможностью оперативного дистанционного контроля и учета факторов изменения параметров окружающей среды. Среди них наибольшее значение имеют группы, связанные со: сдвигом воздушного потока и турбулентности следа, в трех плоскостях, поверхностного скольжения и обледенения, а также эффективностью средств технического зрения: радио, звукового, лазерного оборудования, камер наблюдения, измерителей скорости, высоты и их производных, а также устойчивостью и управляемостью движения центра масс воздушного судна. В исследованиях последнего времени упор делается на выбор инструментальных методов обнаружения изменения параметров воздушных потоков одного воздушного судна для следующего за ним другого судна, а также естественных процессов в приповерхностном слое над взлетно-посадочной полосой. Однако радары и лидары обладают рядом ограничений по надежности обнаружению вихревых образований на требуемом расстоянии и не могут быть использованы как основное средство информирования экипажа судна о вихревой опасности. Проблема состоит в отставании развития радиоэлектронного оборудования для обеспечения эффективности использования взлетно-посадочной полосы при вихревой безопасности заданного уровня. Предметом — является информационная автоматизированная система обеспечения эффективности использования взлетно-посадочной полосы при вихревой безопасности заданного уровня. Объектом исследования являются аппаратно-программные средства автоматизированной системы управления воздушным движением.

Целью работы является повышения эффективности использования взлетно-посадочной полосы за счет повышения безопасности путем расширения измеряемых параметров объектов и окружающей их среды, с их помощью оценки степени угрозы и поддержки принятия решений командиром судна или диспетчером или системой автоматического управления. Актуальность заключается в отсутствии дистанционно измеряемой, оперативной и достоверной информации о динамике системы воздушного судна и окружающей среды достаточной для принятия обоснованных автоматических решений.

Анализ функций, задач, условий и ограничений для бортового оборудования судна и аэродромного комплекса показал необходимость повышения значимости критериев: время реакции судна динамики от обнаружения, измерения, оценки степени угрозы до момента начала эволюции реагирования; пропускная способность радиоканалов, действующих в условиях множества одновременно работающих информационных каналов мониторинга среды, объектов и обмена информацией; помехоустойчивость и помехозащищенность от естественных и преднамеренных помех; точностные характеристики обнаружения и распознавания объектов, явлений и их меняющихся параметров; высока степень значимости ошибочных решений по обнаружению и измерению; отсутствие информационного обеспечения по распознаванию предаварийной ситуации эволюции воздушного судна и выработки вариантов управленческих решений лицу их принимающему; согласованность радиоэлектронных средств и наземного оборудования. В работе предложена структура и математическая модель работы автоматизированной системы управления, уточнены параметры, средства и методика расчета рекомендуемых вариантов: курса, скорости и ускорения по вертикали и горизонтали, дистанции и ориентации относительно оси взлетно-посадочной полосы, впереди и сзади идущих воздушных судов. Предлагается изменение структуры управления организацией воздушного движения в аэропорту до полной связанности и включение в состав оборудования воздушных судов в районе аэропорта, способных к измерению вихревых следов с о стороны, позволяющей получить в отраженном сигнале доплеровское преобразование с радиального, а не тангенсального направления. Штатное оборудование не позволяет достоверно обнаруживать вихри и нарастание сдвигов ветра, обладающие слабой отражающей способностью в условиях отсутствия адаптации к помехам от местных предметов. Для снижения влияния данного фактора предлагается отраженные сигналы рассматривать в областях частотно-временных спектров, в которых устойчиво наблюдаются эффекты расширение спектра, уменьшения времени раскорреляции, что позволяет произвести обнаружение и измерение формы и уровней пространственного эхо-портрета. Изменчивость радиоканала и высокий уровень отражения от среды и местных предметов не позволяют получить требуемые характеристики по измерению параметров вихревых образований и ВС генератора вихрей для определения порога для принятия решения для ухода на второй круг. Применение тестирование канала в реальном масштабе времени позволит адекватно угрозе формировать порог при заданном уровне безопасности и требуемых ресурсов. Автоматизированная информационная система управления подвержена внешним деструктивным воздействиям. Для снижения влияния данного фактора предлагается применение скрытных, разведзащищенных каналов связи, а также применение антивирусных и блокчейн технологии. В работе приведено обоснование необходимости изменение структуры и функций системы управления и организации воздушным движением при посадке воздушного судна, основанной на результатах измерения параметров окружающей среды, в первую очередь сдвига ветра и вихревых процессов с применением радаров дистанционного зондирования как с борта воздушного судна на

глиссаде, так других воздушный судов в районе аэропорта, а также с земли и их комплексного использования. Результаты работы позволят создать предпосылки для разработки методов и средств повышения эффективности использования воздушных судов и взлетно-посадочной полосы при заданном уровне безопасности воздушного движения, за счет увеличения измеряемых параметров и их точности для надежной оценки степени угрозы и алгоритмов принятия решений управляющего воздушным судном.

Ключевые слова: воздушное судно, сдвиг ветра, радар, скорость, дальность.

ИСПОЛЬЗОВАНИЕ СИНТЕТИЧЕСКИХ ТЕСТОВ ДЛЯ ОЦЕНКИ ПРОИЗВОДИТЕЛЬНОСТИ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Кудро Дмитрий Викторович

кандидат технических наук,
Военно-космическая академия имени А.Ф.Можайского,
г. Санкт-Петербург, Россия, kudro@list.ru

Топорков Николай Святославович

Военно-космическая академия имени А.Ф.Можайского,
г. Санкт-Петербург, Россия, k.toporkov@mail.ru

При обосновании выбора вычислительных систем в специальных задачах в настоящее время используются различные методы, позволяющие оценивать характеристики процессов и полноты использования вычислительных ресурсов. Основу для сравнения различных типов вычислительных систем между собой дают стандартные методики измерения производительности. В процессе развития вычислительной техники появилось несколько стандартных методик. Наиболее распространенными методиками измерения производительности вычислительных систем на практике являются методики на основе тестов производительности

Тесты производительности (англ. benchmarks) – это тесты, измеряющие производительность систем, или подсистем на основе решения заранее определенных задач или наборов задач. В настоящее время существует достаточно большой выбор тестов, оценивающих различные аспекты производительности универсальных систем и подсистем.

Применение для оценки производительности автоматизированных систем управления специального назначения существующих универсальных тестов в большинстве случаев, не представляется возможным. Существующие универсальные тесты не отражают специфику задач применения автоматизированных систем управления специального назначения: вычисления, как правило, связаны с интенсивными вычислениями над вещественными числами – коммерческие приложения более критичны к производительности работы с целочисленной арифметикой и обработкой транзакций баз данных. Другие характеристики требуются при оценке графических приложений, отражающей не только вычислительные мощности, но и параметры

самой графической системы или при необходимости оценки необходимой производительности при параллельной и распределенной обработке.

При разработке, испытаниях и обосновании выбора вычислительных систем для автоматизированных системах управления специального назначения, и при совершенствовании конфигурации и режимов функционирования систем, находящихся в эксплуатации, возникает необходимость оценивать производительность на реальных специальных прикладных программах. Однако для оценки и сравнения производительности автоматизированных системах управления использование, например, времени выполнения реальных программ в качестве средства измерения зачастую затруднительно. В связи с этим разработка специализированных синтетических тестов, использующих в качестве эталонных функций различные алгоритмы прикладных программ автоматизированных систем управления специального назначения, которые будут наиболее точно отражать специфику решаемых задач, достаточно актуальна.

В настоящее время для автоматизированных системах управления специального назначения наиболее характерными и в тоже время ресурсоемкими задачами являются:

– обработка радиолокационных и оптических видовых данных;

– прикладные электродинамические расчеты;

– обработка метеорологической информации и моделирование различных атмосферных явлений;

– прикладная баллистика;

– решение несобственных задач линейного программирования большой размерности при эволюционирующей системе данных (оптимальное управление, планирование боевого применения сил и средств);

– моделирование структур и свойств материалов (компьютерное моделирование свойств специальных сплавов, анализ деформирования и возможного разрушения конструкций, исследование процессов разрушения в конструктивных элементах космических аппаратов);

– моделирование процессов распространения радиоволн в различных условиях и сложных технических систем;

– построение параллельных систем баз данных для иерархических кластерных архитектур и др.

При разработке специализированных синтетических тестов предлагается использовать в качестве набора эталонных функций ресурсоемкие алгоритмы, использующиеся при решении приведенных характерных задач, решаемых в автоматизированных системах управления специального назначения. Для комплексного оценивания вычислительных систем в набор эталонных функций необходимо включить алгоритмы реализующие базовые операции, такие как, подпрограммы линейной алгебры, векторные математические функции, векторные функции преобразования и статистики, тригонометрические функции и др. Необходимо предусмотреть импортирование кодов специализированных синтетических тестов на разные платформы, инструментальные средства для формирования осмысленных рабочих нагрузок.

В докладе рассматривается использование эталонной функции оценивания производительности автоматизированных системах управления специального назначения, предназначенного для обработки радиолокационных и оптических данных, как одного из элементов специализированных синтетических тестов. В основе эталонной функции формирования показателя производительности используется алгоритм обработки радиолокационных и оптических данных. Результаты прогона каж-

дого теста выражаются отношением времени выполнения одной копии теста на тестируемой машине к времени ее выполнения на эталонной машине. Таким образом за основу для измерения производительности в данном случае принимается мера относительного времени. Необходимо учитывать, что существует, так называемое «чистое», процессорное время, определяемое как период работы собственно процессора и время выполнения операций ввода/вывода.

Ключевые слова: тесты производительности; автоматизированные системы управления специального назначения; специализированные синтетические тесты.

К ВОПРОСУ СОВЕРШЕНСТВОВАНИЯ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ ДОЛЖНОСТНЫХ ЛИЦ ПРИ ВЕДЕНИИ ВОИНСКОГО УЧЕТА

Смирнов Борис Петрович

доктор технических наук,
закрытое акционерное общество «Научно-производственный центр информационных региональных систем»,
Московская обл., г. Люберцы, Россия, smirnov@npcirs.ru

Зверев Александр Борисович

закрытое акционерное общество «Научно-производственный центр информационных региональных систем»,
Московская обл., г. Люберцы, Россия, zverev@npcirs.ru

Важнейшим элементом системы поддержания ВС РФ на требуемом уровне боевой и мобилизационной готовности является система воинского учета, под которой следует понимать государственную систему регистрации призывных и мобилизационных людских ресурсов, в рамках которой осуществляется комплекс мероприятий по сбору, обобщению и анализу сведений об их количественном составе и качественном состоянии.

Проведенный анализ позволил сделать вывод о том, что в современных условиях развития государства наблюдается негативная динамика снижения количественно-качественных показателей полноты и достоверности воинского учета. Об этом свидетельствуют результаты проведенных в период с 2014 по 2020 годы учений, в ходе которых осуществлялась проверка готовности военных комиссариатов к проведению мобилизации людских и транспортных ресурсов.

На основе изложенного можно сформулировать следующую проблемную ситуацию: под действием ряда деструктивных факторов количественно-качественные характеристики системы воинского учета находятся на низком уровне, что может привести к срыву выполнения задач, возложенных на должностных лиц организационно-мобилизационных органов (далее — оргмоборганов) ВС РФ в мирное и военное время.

Одним из перспективных направлений разрешения проблемной ситуации, не требующим существенных финансовых, материальных и людских ресурсов, является

повышение эффективности функционирования системы воинского учета за счет совершенствования информационного обмена сведениями и документами между должностными лицами военных комиссариатов, органов государственной власти, органов местного само-управления, организаций (далее –должностными лицами) и гражданами посредством системы межведомственного электронного взаимодействия (далее – СМЭВ). Реализация данного информационного обмена может быть осуществлена на основе выбора рационального варианта модели информационного взаимодействия должностных лиц при ведении воинского учета.

Для выбора рациональной модели информационного взаимодействия должностных лиц при ведении воинского учета необходимо решить три взаимосвязанных задачи:

оценки альтернативных вариантов с учетом качественных показателей на основе метода анализа иерархий;

оценки альтернативных вариантов с учетом количественных показателей, в основу которой может быть положен один из методов решения многокритериальных задач;

комплексной оценки и выбора рационального варианта, предусматривающих интегральную свертку качественных и количественных показателей для получения единого обобщенного показателя.

Реализация модели информационного взаимодействия с использованием СМЭВ позволит существенно повысить количественно-качественные показатели полноты и достоверности воинского учета, что, в свою очередь, позитивно отразится на эффективности выполнения задач, возложенных на должностных лиц оргмоборганов ВС РФ, в мирное и военное время.

Ключевые слова: воинский учет; эффективность; информационный обмен; систему регистрации.

НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ, ПРИМЕНЯЕМОЙ В ИНТЕРЕСАХ ОРГАНИЗАЦИОННО-МОБИЛИЗАЦИОННЫХ ОРГАНОВ ВС РФ

Смирнов Борис Петрович

доктор технических наук,
закрытое акционерное общество «Научно-производственный центр информационных региональных систем»,
Московская обл., г. Люберцы, Россия, smirnov@npcirs.ru

Зверев Александр Борисович

закрытое акционерное общество «Научно-производственный центр информационных региональных систем»,
Московская обл., г. Люберцы, Россия, zverev@npcirs.ru

Анализ функций, выполняемых в настоящее время специалистами организационно-мобилизационных органов ВС РФ с использованием автоматизированной системы управления (далее — АСУ) специального назначения позволил сделать вывод о том, что данная АСУ выполняет в основном роль информационно-расчетно-справочной системы, а принятие решений по вопросам планирования и управления призывными и мобилизационными ресурсами остается прерогативой должностных лиц.

Такое состояние дел открывает большие перспективы существенного повышения эффективности применения имеющихся ресурсов за счет развития АСУ в части разработки принципиально нового алгоритмического и программного обеспечения, позволяющего в автоматическом режиме формировать альтернативные варианты возможных решений, проводить их военно-экономическую оценку и предлагать должностным лицам оптимальные варианты решения стоящих перед ними задач. По сути, дальнейшее развитие АСУ должно идти по пути разработки математических моделей поддержки принятия решений (далее — ММППР) и их реализации в существующих и перспективных программных средствах.

Решение данной задачи должно осуществляться поэтапно:

на первом этапе в рамках НИР целесообразно разработать комплекс математических моделей, методик и алгоритмов решения оптимизационных задач с целью повышения эффективности применения имеющихся призывных и мобилизационных ресурсов, а также оценить реальный вклад от реализации разработанного научно-методического аппарата в повышение боевой и мобилизационной готовности войск;

на втором этапе в рамках ОКР необходимо разработать программное и информационно-лингвистическое обеспечение для реализации созданных на первом этапе математических моделей поддержки принятия решений.

Научно-исследовательские работы позволят разработать модели, методики и алгоритмы решения оптимизационных задач:

– мобилизационного планирования и управления;

– планирования и управления призывными ресурсами;

– планирования и управления подготовкой должностных лиц к работе с АСУ;

– планирования и управления оснащением и переоснащением техническими и программными средствами.

В области мобилизационного планирования и управления значительный практический интерес представляют обоснования оптимальных планов:

– предназначения мобилизационных людских ресурсов на воинские должности;

– предназначения техники, поставляемой в воинские части по мобилизационному плану, в военных комиссариатах;

– восполнения некомплекта людских ресурсов и техники в ходе выполнения мобилизационных мероприятий;

– подготовки специалистов в ходе проведения сборов в условиях ограничений на общее количество обучаемых.

В области планирования и управления призывными ресурсами целесообразно сосредоточить внимание на решении сложных прикладных задач обоснования:

– распределения призывников в виды и рода ВС РФ, соединения и воинские части по результатам первоначальной постановки на воинский учет;

– распределения призывников по должностям и военно-учетным специальностям (далее – ВУС) в воинской части с учетом их уровня образования и других характеристик;

– распределения призывников по специальностям для подготовки в учебных частях;

– распределения специалистов в виды и рода ВС РФ, соединения и воинские части после окончания обучения в учебных частях;

– распределения специалистов по должностям и ВУС в воинской части после окончания обучения в учебных частях с учетом их уровня образования и других характеристик.

В областях планирования и управления подготовкой должностных лиц к работе с АСУ, оснащением и переоснащением техническими и программными средствами уже выполнено достаточно качественных НИОКР.

В докладе приведен лишь небольшой круг оптимизационных задач, решение которых позволит существенно повысить эффективность деятельности должностных лиц оргмоборганов ВС РФ по рациональному применению призывных и мобилизационных ресурсов. После проведения соответствующего экспертного опроса должностных лиц организационно-мобилизационных органов разных уровней данный перечень задач может существенно расшириться.

Ключевые слова: автоматизированная система управления; информационно-расчетно-справочная система.

НЕЙРОСЕТЕВОЙ ПОДХОД К ПОСТРОЕНИЮ МАРШРУТА В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Данильченко Михаил Николаевич
кандидат технических наук, АО «Концерн «Созвездие»,
г. Воронеж, Россия, m.n.danilchenko@sozvezdie.su

Современный этап развития инфокоммуникационных систем (ИКС) и технологий характеризуется их быстрым ростом и усложнением, вызванным повышением требований потребителей к скорости и качеству обмена информацией. Этим обусловлена актуальность задач по обеспечению эффективного использования сетевых ресурсов. Одна из ключевых таких задач – задача построения оптимальных маршрутов в ИКС, качественная новизна которой в современных условиях обусловлена резко возросшей мобильной компонентой современных ИКС и стремительным ростом значения принципов самоорганизации, применяемых для их управления. Таким образом, управление современными ИКС становится не только автоматизированным, но и динамическим и адаптивным, а сам объект управления – самоорганизующимся.

Настоящий доклад посвящен анализу перспективного подхода к решению задачи динамической маршрутизации с учетом состояния каналов в автоматизированной системе управления специального назначения с использованием искусственной нейронной сети (ИНС) Хопфилда.

Преимуществом данного подхода является вариативность построения маршрута между парой абонентов в сети, заложенная в рассматриваемом алгоритме. Выявленный факт предоставляет потенциальные возможности равномерного распределения нагрузки в каналах, чего не обеспечивают оптимальные алгоритмы, в частности алгоритм Дейкстры. Кроме того, наличие указанного свойства обеспечивает возможность снижения накладных расходов, связанных с необходимостью организации служебного трафика для обновления информации о состоянии сети при реализации протоколов маршрутизации.

В связи с этим основополагающей задачей для использования нейронных сетей Хопфилда при построении маршрута в реальных инфокоммуникационных системах является формирование критерия останова процесса эволюции сети, который позволит корректно оценить время работы алгоритма, а также эффект, получаемый от применения рассмотренного алгоритма на интегральные показатели системы.

При описании используемого метода построения маршрута в автоматизированной системе, модифицируется энергетическая функция Ляпунова, идентифицирующая состояние ИНС Хопфилда. В докладе дан окончательный вид энергетической функции в виде пяти слагаемых, описана зависимость, определяющая динамику изменения входов ИНС Хопфилда, разработана структурная схема алгоритма функционирования ИНС для формирования маршрута в ИКС.

Ключевые слова: алгоритм построения маршрута; сеть Хопфилда; энергия сети Хопфилда; динамическая система; вес связи нейрона; смещение нейрона; кратчайший путь.

ПРОГНОЗИРОВАНИЕ РАСПРЕДЕЛЕННЫХ ВО ВРЕМЕНИ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Королев Игорь Дмитриевич
доктор технических наук, профессор,
Краснодарское высшее военное училище
имени генерала армии Штеменко С.М.,
г. Краснодар, Россия, pi_korolev@mai.ru

Попов Владимир Игоревич
Краснодарское высшее военное училище
имени генерала армии Штеменко С.М. ,
г. Краснодар, Россия, ya28vip@mail.ru

Крюков Денис Матвеевич
Краснодарское высшее военное училище
имени генерала армии Штеменко С.М.,
г. Краснодар, Россия, isas2010@mail.ru

Исходя из принципов реализации выявления компьютерных атак и поиска скрытых закономерностей их реализации, существует ряд тенденций не только на ложные срабатывания системы, но и на пропуск реальных инцидентов информационной безопасности. Наиболее адекватным методом выявления инцидентов информационной безопасности при анализе скрытых закономерностей является метод прогнозирования поведения системы. Для анализа скрытых закономерностей имеется база данных с последовательными цепочками событий информационной безопасности, появление которых не всегда является последовательным. В ряде случаев, для взлома системы и проникновения в нее обходными путями, противник создает все более изощренные способы для реализации своих умышленных намерений. Также существует сеть, основанная на намерениях, которая добавляет пользовательский контекст, способный обучить ее, создавая возможности обеспечения контроля, тесно связывая политику безопасности с намерениями пользователя. Добавляя эти важные возможности, сетевая платформа с замкнутым циклом, основанная на намерениях, помогает специалисту по информационной безопасности обеспечить непрерывную гибкость, надежность и безопасность системы. Для реализации умышленных намерений противнику необходимо достигнуть своей цели. Исходя из известных методов выявления компьютерных атак, он будет строить обходные пути для достижения цели. Современные системы обнаружения атак построены на выявлении инцидентов информационной безопасности с использованием сигнатурного и поведенческого метода (эвристического подхода), но не предусматривают комбинацию обхода данных методов путем реализации атаки по нескольким незавершенным цепочкам событий информационной безопасности. Для выявления подобных угроз информационной безопасности необходимо использовать методы прогнозирования. Предсказание будущего с помощью научных методов – есть прогнозирование конкретных перспектив развития ситуации или процесса. Существует множество методов и способов прогнозирования развития процессов, которые имеют как ряд преимуществ, так и недостатков. Для прогнозирования проведения компьютерной атаки по незавершенным цепочкам событий информационной безопасности, а также реализации умышленных намерений противника, необходим анализ скрытых закономерностей

данных цепочек событий информационной безопасности, в которой имеются незавершенные цепочки событий информационной безопасности и одиночные события информационной безопасности, исходя из реализации которых, необходимо оценить дальнейшие действия злоумышленника. Базу данных реализуют в многомерном представлении, определив при этом соответствующие кластеры для каждого события информационной безопасности, где кластер – это набор завершенных цепочек, объединенных по какому-либо признаку. При обнаружении очередного события информационной безопасности в заданном кластере отображается соответствующий набор нулей и единиц. Создают многомерное двоичное кластерное пространство размерностью в N всех цепочек событий информационной безопасности, в котором Z кластеров. Априорные вероятности знаний о потенциальном нарушителе дают нам конфигурацию многомерного двоичного кластерного пространства и размещенных в нем кластеров завершенных цепочек событий информационной безопасности. Пусть дано одиночное событие информационной безопасности. Необходимо оценить вероятность завершения цепочки для этого одиночного события информационной безопасности. Исходя из того, что в многомерном двоичном кластерном пространстве Z кластеров, вычислим расстояние d_z. Для чего вычислим расстояние от x до всех завершенных цепочек событий информационной безопасности данного кластера. Расстояние d_z необходимо измерять по метрике Хэмминга, то есть измерить число позиций между двумя двоичными последовательностями x и y длины n, в которых они различны, тогда минимальное расстояние кода равно наименьшему из всех расстояний по Хэммингу между различными парами кодовых слов. Далее находят наиболее всего вероятностный кластер k с расстоянием до него d_k, а также среднее расстояние до всех остальных кластеров. Очевидно, что отношение среднего расстояния и расстояния d_k находится в пределах от 1 до N. Далее определяют диапазон значений от 0 до 1. Тем самым, получая формулу вероятности, которая будет связана с расстоянием. Чем меньше расстояние по метрике Хэмминга от одиночного события информационной безопасности до незавершенной цепочки событий информационной безопасности в рассматриваемом многомерном двоичном кластерном пространстве, тем больше вероятность обнаружения инцидента информационной безопасности, в соответствии с вычисленным коэффициентом корреляции. При анализе и выявления скрытых закономерностей компьютерных атак наиболее адекватным методом является прогнозирование поведения системы. Многомерная база данных инцидентов информационной безопасности, разбитая на двоичное кластерное пространство, помогает реализовать подсчет минимального расстояния от незавершенной цепочки событий информационной безопасности до одиночного события информационной безопасности, а также подсчитать вероятности перехода атаки на различных уровнях в соответствии с коэффициентом корреляции, характеризующий отклонение зависимости между длинами переходов по вертикали (уровнями) и по горизонтали (цепочками) в метрике Хэмминга. Благодаря этому расчету можно сделать вывод о том, о каком инциденте информационной безопасности идет речь: о продолжении старого, либо о реализации нового.

Ключевые слова: инцидент информационной безопасности; событие информационной безопасности; система мониторинга угроз информационной безопасности; прогнозирование инцидентов информационной безопасности; многомерная база данных.

СЕКЦИЯ № 2

МАТЕМАТИЧЕСКОЕ, ПРОГРАММНОЕ И ИНФОРМАЦИОННО-ЛИНГВИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

АНАЛИЗ ДЕЯТЕЛЬНОСТИ БИБЛИОТЕКИ АЛГОРИТМОВ И ПРОГРАММ

Яшенков Николай Николаевич

кандидат технических наук,
27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, nikolaiyashenkov@rambler.ru

Иванов Владимир Владимирович

27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, popovka2108@gmail.com

Яшенкова Марина Александровна

27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, nik.yashenkov@yandex.ru

За последние десятилетия, начиная с 90-х годов XX века, получен достаточно большой положительный опыт в военно-научном сопровождении создания образцов программной продукции различного назначения. Однако существует ряд факторов, снижающих качество их разработки:

1) отсутствие единой политики создания программной продукции и общей координации разработок в интересах получения системных решений;

2) технологическая несовместимость программных решений, используемых в различных автоматизированных системах;

3) невыполнение требований государственных образовательных стандартов предприятиями промышленности, приводящее к разработке некачественной программной продукции.

Вместе с тем, на данный момент эксплуатируется большое количество программной продукции различного назначения. При этом ее эксплуатация ограничена областью применения и не всегда отвечает предъявляемым к ней требованиям (особенно в части документации). Следует отметить, что математический аппарат программной продукции позволяет обеспечивать выполнение необходимых функций с достаточно высоким качеством, однако, из-за бессистемного, автономного проекти-

рования, отсутствия унификации данные программные средства зачастую не соответствуют требованиям практики (в первую очередь оперативности).

Библиотека алгоритмов и программ представляет собой систему формирования, хранения и ведения задач и моделей, функционирующую в соответствии с действующим законодательством Российской Федерации и на основании своего положения, определяющего назначение, состав, организационную структуру, порядок ее формирования, ведения, использования и развития.

Анализ деятельности библиотеки алгоритмов и программ показал, что ее ведение позволяет решить проблемы в части:

– проведения единой научно-технической политики в области разработки, внедрения и использования программной продукции;

– обеспечения разработчиков и потребителей программной продукции информацией о задачах и моделях, разработанных и/или закупаемых по заказам;

– повышения эффективности разработки и использования программной продукции, устранения дублирования разработок и необоснованных закупок;

– оказания научно-технических консультаций пользователям программной продукции.

Ключевые слова: библиотека алгоритмов и программ, функционирование, программная продукция, анализ деятельности, факторы, качество разработки, внедрение и использование.

МАРШРУТИЗАЦИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ, ТРАНСЦЕНДЕНТНЫЕ ЦЕЛЕВЫЕ ФУНКЦИИ ГРАФА И ГЕНЕТИЧЕСКИЙ АЛГОРИТМ

Руденко Эдуард Михайлович

кандидат технических наук,
филиал Военной академии Ракетных войск стратегического назначения
имени Петра Великого, г. Серпухов, Россия, eduard5529@yandex.ru

Семикина Елена Викторовна

филиал Военной академии Ракетных войск стратегического назначения
имени Петра Великого, г. Серпухов, Россия, labinfo_serp@inbox.ru

Рассматривается задача поиска маршрутов беспилотных летательных аппаратов на различных графах реперных точек на местности с использованием генетического алгоритма. Проводится сравнение методов построения целевой функции графа на основе алгебраического, теоретико-числового подхода, а также с использованием трансцендентных функций. Рассмотрение примеров целевых функций, построенных алгебраическими методами с учетом кратности номеров вершин в замкнутом маршру-

те, показывает, что такой подход приводит для графов большой размерности к ложным маршрутам. Указанный недостаток можно устранить, учитывая индивидуальную информацию о каждом ребре графа. Это обеспечивается кодированием ребер графа слагаемыми или сомножителями некоторой числовой величины в виде ее однозначного разложения. Построение целевой функции опирается при этом на теоретико-числовые свойства s-ического разложения или на разложение целого числа на простые множители. Теоретико-числовые целевые функции однозначно учитывают индивидуальность каждого ребра. Такое кодирование ребер позволяет сформулировать теорему построения целевых функций на графах, основанную на однозначном разложении числовой величины в сумму или произведение. Дальнейшие исследования показывают, что в качестве числовых кодов могут быть использованы не только числа, но и функции, которые более полно отражают информацию об индивидуальных особенностях задачи маршрутизации на графах и тоже обладают свойствами однозначного разложения. Сочетание свойств кода быть числом и функцией приводит к его трансцендентности и возможности применения в построении целевой функции. Проводится апробирование построенных трансцендентных целевых функций на примерах различных графов. Показана взаимосвязь прикладной задачи маршрутизации беспилотных летательных аппаратов на местности с математической задачей оптимизации на графах средствами теории чисел и генетического алгоритма. Рассмотрено обобщение кодирования ребер и вершин графа в метод построения трансцендентных целевых функций. Трансцендентные целевые функции строятся на основании однозначного представления любой математической величины как суммы независимых слагаемых или произведения неприводимых множителей. Дуализм представления кодов ребер и вершин графа в числовой и функциональной форме открывает направление применения в автоматизированных системах управления генетического алгоритма для выбора контуров управления, как маршрутов на графе.

Ключевые слова: маршрутизация; графы; алгебраические целевые функции; теоретико-числовые целевые функции; трансцендентные целевые функции; генетический алгоритм.

МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОПТИМИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ

Пасечник Родион Маратович

*Краснодарское высшее военное училище имени генерала армии Штеменко С.М.,
г. Краснодар, Россия, rmpasechnik@mail.ru*

Табункова Марина Павловна

*Краснодарское высшее военное училище имени генерала армии Штеменко С.М.,
г. Краснодар, Россия, skygel@mail.ru*

Королёв Игорь Дмитриевич

*Краснодарское высшее военное училище имени генерала армии Штеменко С.М.,
г. Краснодар, Россия, pi_korolev@mail.ru*

Обеспечение защиты информационно-телекоммуникационных сетей и информационных систем значимых объектов критической информационной инфраструктуры Российской Федерации диктует необходимость учёта множества внутренних и внешних факторов влияющих на достаточный уровень защищенности. Преобразование характера угроз информационной безопасности затрудняет процесс решения задач должностными лицами органов системы обнаружения предупреждения и ликвидации последствий компьютерных атак. Этот аспект справедливо должен быть компенсирован таким комплексом средств защиты информации, который бы надежно перекрывал все возможные уязвимости с одной стороны и соответствовал действующим нормативным документам, регламентирующим меры обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры — с другой. Ограниченность ресурсов, в том числе материальных, непрерывное преобразование угроз информационной безопасности и связанные с этим сложности формируют соответствующую научно-техническую проблему и остро ее актуализируют.

Формирование рациональной подсистемы защиты информации в автоматизированных системах предполагает наличие множества вариантов конфигураций, состоящих из множества средств защиты информации (далее – средств) и дальнейший выбор из этого множества оптимального варианта построения комплекса средств по определенным критериям. Для этого необходимо определить и обосновать круг особенностей, которые должны быть учтены при математической постановке задачи. К их числу относятся:

– перечень и оценка уязвимостей информационной безопасности изложены и утверждены MITRE. Основание для использования данной базы продиктовано ее полнотой, оперативностью пополнения и отсутствием равноценной отечественной альтернативы;

– перечень технических мер обеспечения информационной безопасности значимого объекта критической информационной инфраструктуры должен в достаточной степени гарантировать нейтрализацию всех уязвимостей базы MITRE. В данном случае под исчерпывающим перечнем технических мер будет пониматься состав мер по обеспечению информационной безопасности для значимого объекта соответствующей категории значимости, установленный приказом ФСТЭК России №239 от 25 декабря 2017 г. «Об утверждении Требований по обеспечению безопасности зна-

чимых объектов критической информационной инфраструктуры Российской Федерации»;

– количество перекрытий одной и той же меры разными средствами из комплекса должно быть минимальным. Это продиктовано стремлением к экономизации материальных ресурсов;

– комплекс должен состоять из средств с максимально высокими оценками. Определение оценки средства заключается в нахождении отношения суммы оценок тех мер, которые оно закрывает, к сумме оценок всех мер, определенных приказом Федеральной службы по техническому и экспортному контролю России. В свою очередь, для получения оценки меры необходимо найти значение отношения суммы оценок уязвимостей, которые данная мера перекрывает к сумме оценок всех уязвимостей, которые отражены в MITRE. Так, оценка меры строится на количестве уязвимостей, которые нейтрализуются данной мерой, а также на критичности этих уязвимостей;

– для технической реализации системы должно выполняться условие совместимости, которая производится в тех случаях, когда совместимость между подсистемами защиты информации предусмотрена. Для этого необходимо построить граф совместимости подсистем защиты информации;

– время развертывания системы должно лимитироваться в зависимости от периода и целей создания системы защиты информации и формирования оптимального комплекса средств на значимом объекте критической информационной инфраструктуры;

– должны быть определены пороговые значения стоимости формируемого комплекса средств для значимого объекта критической информационной инфраструктуры в зависимости от ряда параметров, таких как: размер финансирования организации; масштаб организации и прочие затраты ресурсов. Сюда же должны быть включены сопутствующие затраты на: возможное обучение/переобучение работников, связанное с установкой новых средств; покупку лицензий; платную техническую поддержку и другие затраты, неотделимые от самого средства и без которых работоспособность данного средства может быть поставлена под сомнение;

– количество средств в комплексе должно стремиться к минимуму для сокращения степени риска, связанного с силами, требуемыми для управления и контроля над работоспособностью каждого средства.

Таким образом, по каждому пункту, отражающему особенности построения оптимального комплекса средств дано краткое обоснование причин, по которым следует его учитывать при постановке и решении задачи оптимизации. Приведенная методика является частным случаем классической оптимизационной задачи. Формализация и обоснование особенностей применения средств позволили сформулировать целевую функцию и соответствующие ограничения, что в конечном итоге существенно повышает эффективность составления комплекса средств с точки зрения перекрытия всех уязвимостей и использования при этом всех мер, предусмотренных действующим законодательством.

Ключевые слова: комплекс средств защиты информации; система обнаружения, предупреждения и ликвидации последствий компьютерных атак; база MITRE; оценка уязвимостей; меры защиты информации; совместимость средств защиты информации; оценка меры обеспечения безопасности.

МЕТОДИКА АВТОМАТИЧЕСКОГО КОНТРОЛЯ ОФОРМЛЕНИЯ И ПОДГОТОВКИ ОКОНЧЕННЫХ ЭЛЕКТРОННЫХ ДЕЛ ДЛЯ ПЕРЕДАЧИ НА АРХИВНОЕ ХРАНЕНИЕ

Королев Игорь Дмитриевич

доктор технических наук, профессор,
Краснодарское высшее военное училище имени генерала армии Штеменко С.М.,
г. Краснодар, Россия, pi_korolev@mail.ru

Назинцев Вадим Сергеевич

Краснодарское высшее военное училище имени генерала армии Штеменко С.М.,
г. Краснодар, Россия, lazo12@list.ru

Акинфиев Данил Викторович

Войсковая часть 26977
г. Севастополь, Россия, alhim26@icloud.com

В Российской Федерации, так же как и большинстве развитых стран мира, вопросам долговременного хранения управленческих электронных документов уделяется большое внимание. На государственном уровне принимаются нормативные правовые акты, принимаются национальные и международные стандарты в области делопроизводства и архивного дела.

В настоящее время в Российской Федерации в соответствии со стратегией развития информационного общества в Российской Федерации на 2017–2030 гг., утвержденной указом президента Российской Федерации от 09.05.2017 № 203 активно развиваются и внедряются информационные технологии, как во все сферы государственной деятельности, так и во все сферы деятельности граждан. Создана система предоставления государственных и муниципальных услуг в электронной форме, для чего на всех уровнях органов исполнительной власти внедряются информационные системы, в том числе и системы электронного документооборота. В соответствии с требованиями Правил делопроизводства в государственных органах, органах местного самоуправления, утвержденных приказом Федерального архивного агентства от 22 мая 2019 года все документы, поступающие в государственные органы, органы местного самоуправления на бумажном носителе информации переводятся в электронный вид и хранятся в информационных системах. При этом электронный документооборот государственного органа осуществляется с помощью системы электронного документооборота.

Это привело к взрывному росту объема электронных документов, обрабатываемых в информационных системах государственных органов, органов местного самоуправления, возникновению необходимости повышения оперативности их обработки, интегрированию существующих информационных систем с СЭД в целях реализации функции отбора документов временных (свыше 10 лет) и постоянного сроков хранения для передачи на хранение в архив государственного органа, органа местного самоуправления и выделения к уничтожению документов, сроки хранения которых истекли. В связи с этим актуальной научной задачей является разработка методик выполнения процессов в информационных системах, позволяющих повысить оперативность обработки информации.

Одним из процессов делопроизводства является процесс контроля оформления оконченных электронных дел и подготовки их для передачи на архивное хранение.

Анализ функциональных возможностей наиболее распространенных в государственных органах, органах местного самоуправления систем электронного документооборота показал, что выполнение процесса контроля оформления оконченных электронных дел и подготовки их передаче на архивное хранение не реализован, и выполняется путем выполнения интеллектуальной деятельности оператором автоматизированного рабочего места системы электронного документооборота.

Для решения задачи повышения оперативности обработки информации в системе электронного документооборота разработана методика автоматического контроля оформления оконченных электронных дел для их передачи на архивное хранение. Методика автоматического контроля оформления оконченных электронных дел для их передачи на архивное хранение состоит из: способа автоматического контроля присвоения реквизитов оконченному электронному делу; способа автоматического контроля заполнения описи электронных дел; способа сбора информации об операциях, проводимых с электронными делами; способа автоматического контроля заполнения сопроводительной документации на электронные дела, передаваемые на архивное хранение.

Способ автоматического контроля присвоения реквизитов оконченному электронному делу заключается в осуществлении контроля заполнения полей учетной формы оконченных электронных дел и корректности, занесенных в них значений, при наступлении системной даты в системе электронного документооборота первое января года, следующего за годом заведения электронного дела таких как: индекс электронного дела, наименование электронного дела, мандатная метка электронного дела, дата начала электронного дела, дата окончания электронного дела, объем информации в электронном деле, срок хранения электронного дела, структурное подразделение (должностное лицо) к чьей области информационной ответственности относится электронное дело.

Способ автоматического контроля заполнения описи электронных дел заключается в осуществлении контроля заполнения полей описи электронных дел и реестра электронных документов, включенных в электронное дело, корректности, занесенных в них значений, при наступлении системной даты в системе электронного документооборота первое января года, следующего за годом заведения таких как: наименования организации, сдающей электронные дела, номер фонда, номер описи, индекс электронного дела, наименование электронного дела, дата начала электронного дела, дата окончания электронного дела, объем информации в электронном деле. Контроль заполнения полей реестра электронных дел: дата электронного документа; регистрационный номер электронного документа; наименование электронного документа; объем электронного документа; формат электронного документа.

Способ сбора информации об операциях, проводимых с электронными делами в системе электронного документооборота в рамках методики вынесен в ограничения и не рассматривался.

Способ автоматического контроля заполнения сопроводительной документации на электронные дела, передаваемые на архивное хранение, заключается в осуществлении контроля заполнения полей сопроводительной документации таких как: наименование электронного дела; дата создания электронного дела; характеристики содержания (аннотации) электронного дела; электронного формата электронного дела; объем электронного дела.

Разработанная методика позволяет повысить оперативность выполнения процесса автоматического контроля оформления и подготовки оконченных электронных дел к передаче на архивное хранение и обработки информации в системах электрон-

ного документооборота в целом. Может быть использована при проектировании перспективных и модернизации существующих систем электронного документооборота, реализована в виде программного модуля, реализующего функцию автоматического контроля оформления и подготовки оконченных электронных дел к их передаче на архивное хранение. Отличается от существующих тем, что модели подпроцессов описаны на языке логики предикатов, применение методики позволит выполнять процесс контроля оформления оконченных электронных дел и подготовки их к передаче на архивное хранение в автоматическом режиме.

Ключевые слова: документооборот; архивное хранение; электронные дела; автоматическое оформление; номенклатура дел, подготовка к сдаче.

МЕТОД КОМПЛЕКСИРОВАНИЯ ДАННЫХ В СИСТЕМЕ РАСПРЕДЕЛЕННОГО МОНИТОРИНГА

Моисеев Александр Александрович

кандидат технических наук,
Научно производственное предприятие «Технос–РМ»,
г. Мытищи МО, Россия, slow.coach@yandex.ru

Современные системы распределенного мониторинга включают устройства наблюдения и регистрации различных типов. Разнородность формируемых ими данных порождает проблемы, связанные:

– с объединением разнородных данных от различных источников, зачастую слабо связанных;

– противоречивостью, неполнотой и неточностью данных в отсутствие априорной идентификации наблюдаемых объектов;

– требованием оперативной обработки большого объема разнородной информации.

В данной работе рассматриваются алгоритмы обработки разнородных данных, обеспечивающие агрегирование последних с целью приведения к обозримому виду, удобному для получения аналитических выводов, повышения их надежности и принятия решений. Предлагаемый подход к комплексированию данных от разнородных источников состоит в использовании объединенного вектора признаков объектов. Дополнительной проблемой при этом является необходимость реализации комплексирования на единой формальной основе. Однако задача настолько назрела, что попытки создания такой основы на базе метода функционального шкалирования представляются вполне оправданными. Внутри этого направления развивается подход, основанный на переходе от исходных показателей к обобщенным, обрабатываемым численными методами. Последние ориентированы на решение следующих задач:

– снижение размерности векторов признаков за счет предварительного отбора наиболее информативных показателей;

– рациональная оцифровка анализируемых признаков;

– разбиение совокупности объектов на некоторое число однородных классов в рамках автоматической классификации без учителя;

– статистический анализ эффективности проведенного разбиения.

Для отображения признаков объекта используются номинальные (бинарные), порядковые (целочисленные) и относительные (действительные) показатели (переменные), нормированные к диапазону (0,1). В работе продемонстрировано преимущество евклидовой и манхэттенской метрик в пространстве нормированных переменных, состоящее в возможности естественным образом сформировать порог различения на базе критерия Неймана-Пирсона. Приведены также примеры формирования переменных различного типа и их использования на практике.

Ключевые слова: распределенный мониторинг; разнородные данные; агрегирование (комплексирование) данных; функциональное шкалирование; евклидова метрика, манхэттенская метрика; критерий Неймана-Пирсона.

МЕТОДЫ ТЕОРИИ ХАОСА ДЛЯ ЗАДАЧ ДИНАМИЧЕСКОГО УПРАВЛЕНИЯ КОНТАКТ-ЦЕНТРАМИ

Гольдштейн Александр Борисович

кандидат технических наук, доцент,
Санкт-Петербургский государственный университет телекоммуникаций имени проф. М.А. Бонч-Бруевича; НТЦ АРГУС,
г. Санкт-Петербург, Россия, agold@niits.ru

Кисляков Сергей Викторович

кандидат технических наук, доцент,
Санкт-Петербургский государственный университет телекоммуникаций имени проф. М.А. Бонч-Бруевича; НТЦ АРГУС,
г. Санкт-Петербург, Россия, s.v.kislyakov@gmail.com

Феноменов Михаил Александрович

НТЦ АРГУС
г. Санкт-Петербург, Россия, m.fenomenov@argustelecom.ru

Контакт-центры сегодня развиваются очень динамично. Причины этому лежат на поверхности. Это и всеобщая «телефонизация + цифровизация», это и объективная необходимость обслуживания большого числа клиентов удалённо. Последнее особенно актуально в наше непростое время пандемии.

Экономика контакт-центров несложная. Одним из основных рычагов оптимизации затрат на его является минимизация ФОТ, что в свою очередь требует минимизации количества отрабатываемого времени операторами. Если учесть необходи-

мость выполнения договора о качестве обслуживания, то есть вполне объективное рассчитываемое число операторов контакт-центра, аналитически получаемого исходя из нагрузки.

Одним из основных показателей, характеризующих обработанные входящие вызовы, является время ожидания клиента в очереди. Этот показатель сильно влияет на общее впечатление от пользования услугами контакт-центра. Считается, что оптимальным значением будет формула 80/20, то есть 80% звонков ожидают обработки менее 20 с.

Еще один важный показатель — это среднее время обработки вызова оператором. Слишком продолжительные обработки вызовов могут говорить о непрофессиональной работе операторов, а слишком короткие — о том, что они реально не предоставляют услуг потребителям. Если вызов не дождется обработки оператором, то услуги клиенту предоставлено не будет. Оптимальным значением этого показателя считается 4–8%.

Оценка удовлетворенности клиентов является наиболее важным показателем и обычно определяется в ходе опросов после вызова, хотя в оценку могут быть включены и другие показатели, такие как, например, Net Promoter Score - Индекс потребительской лояльности.

На все эти показатели так или иначе влияет организация работы самих операторов — работников КЦ — их расписание и их количество в смене. Если операторов будет меньше оптимума, то очередь вырастет и упадёт уровень обслуживания. Если же их будет слишком много, то увеличится время простоя и возрастут потери на оплату труда. Поэтому крайне важно оптимизировать расписание операторов, которое напрямую зависит от входящей нагрузки. Нагрузка же –величина переменная и зависит от целого ряда факторов, например, от времени суток, дня недели и даже погоды.

В документах организации TeleManagement Forum комплекс таких задач определяется как Workforce management (WFM) — управление рабочей силой — это общее название совокупности процессов планирования, результатом которого является расписание для работников на некоторый будущий период. Анализ производится на основе данных о входящем трафике за предыдущие периоды и производительности операторов. Итогом работы становится расписание для каждого оператора контакт-центра.

WFM применительно к контакт-центрам можно разделить на несколько задач:

- Прогнозирование нагрузки на определенных временных интервалах (обычно 15-30 мин);
- Определение количества операторов, и при необходимости операторов с определенной квалификацией, которые должны находиться в определенный временной интервал на рабочих местах;
- Формирование расписания работы сотрудников контакт-центра.

Добиться минимальной ошибки для прогнозирования довольно сложно, т.к. требуется учесть множество факторов, влияющих на поток поступающих вызовов. Для разных профилей бизнеса это могут быть:

- Всплески количества вызовов как результат маркетингового продвижения;
- Изменения спроса — например, приобретение новой компании или появление новых продуктов;
- Погодные факторы — снег, наводнения и очень жаркая погода могут оказать большое влияние на количество поступающих звонков;

• Специальные мероприятия – такие события, как чемпионат мира, могут вызвать большое всплеск звонков;

• Отказы оборудования — отключение питания, обрыв телефонных линий и т.д.

Влияние этих факторов необходимо минимизировать для получения максимально точных результатов прогнозирования.

Для прогнозирования нагрузки в данной работе применялись методы простого нелинейного прогнозирования, локального линейного прогнозирования и глобальной полиномиальной аппроксимации. В работе приводятся и обсуждаются результаты применения этих методов.

Предложенный подход апробирован в платформе Аргус-WFM CC и доказал свою эффективность в ряде Call-центров на сетях связи РФ.

Ключевые слова: контакт-центр; динамическое управление; автоматизация связи; теория хаоса; управление инфокоммуникациями.

МОНИТОРИНГ РАЗРАБОТКИ СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ — СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

Яшенков Николай Николаевич

кандидат технических наук,
27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, nikolaiyashenkov@rambler.ru

Яшенкова Марина Александровна

27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, nik.yashenkov@yandex.ru

Трунина Татьяна Евгеньевна

27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, tatianatr@list.ru

Проблема повышения качества принимаемых решений неразрывно связана с вопросами разработки и совершенствования средств автоматизации, а также их внедрения в деятельность должностных лиц органов управления.

Решение данной проблемы обеспечивается расчетно-аналитической деятельностью должностных лиц на основе применения задач и моделей, входящих в состав

специального программного обеспечения автоматизированных систем различного назначения, а также ведением реестра программной продукции, позволяющего обобщить и систематизировать научно-технический задел, созданный предприятиями промышленности и научными организациями и включающий в себя:

1) сведения о программном средстве;
2) основание для разработки;
3) сведения об организации-разработчике;
4) сведения о документации и постановках;
5) требования к аппаратно-программной платформе, среде разработки и соответствующему программному обеспечению (эксплуатационные потребности);
6) возможности по моделированию:
– тип модели;
– моделируемые процессы;
– учет влияния условий среды;
– выполняемые расчеты;
– тип и количество моделируемых объектов и т.д.
7) возможности по организации работы с моделями:
– входные данные;
– оперативность моделирования;
– визуализация процесса моделирования;
– возможности по документированию процесса моделирования;
– возможности по организации взаимодействия модели с офисными документами;
– возможности по организации взаимодействия модели с внешними автоматизированными системами и т.д.
8) результаты апробации.

Мониторинг разработки специального программного обеспечения на основе достоверных данных позволяет выявлять потребность органов управления в новых разработках, исключать дублирование, что, в свою очередь, позволяет создавать действительно необходимую программную продукцию различного назначения, а должностным лицам органов управления – принимать обоснованные решения на основе данных программных средств, отвечающих требованиям практики и руководящих документов.

Ключевые слова: мониторинг, разработка, специальное программное обеспечение, реестр, состояние, перспективы.

ОБЗОР РЕЗУЛЬТАТОВ РАБОТЫ С ПРЕДПРИЯТИЯМИ ПРОМЫШЛЕННОСТИ ПО ОТБОРУ И ИСПОЛЬЗОВАНИЮ СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Яшенков Николай Николаевич

кандидат технических наук,
27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, nikolaiyashenkov@rambler.ru

Иванов Владимир Владимирович

27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, popovka2108@gmail.com

Яшенкова Марина Александровна

27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, nik.yashenkov@yandex.ru

В настоящий момент одной из важных задач в Вооруженных Силах Российской Федерации является обобщение и систематизация научно-технического задела, созданного предприятиями промышленности в области создания и применения специального программного обеспечения.

В рамках решения задачи организована работа с предприятиями промышленности, проведена оценка специального программного обеспечения в соответствии с утвержденной методикой.

В ходе оценки учитывались следующие параметры:

– совокупность моделируемых процессов — суммируемая количественная оценка частных показателей, описывающих процессы моделирования в различных областях применения;

– учет внешних условий и факторов — суммируемая количественная оценка частных показателей, отражающих возможность учета условий и факторов в процессе моделирования;

– возможность совершенствования и наращивания программных средств — количественная оценка, представляющая собой совокупность сведений по возможностям модернизации алгоритмов, реализованных в специальном программном обеспечении, по наличию программных интерфейсов, обеспечивающих взаимодействие с внешними системами моделирования, а также по наличию сертификата и комплекта пользовательской документации;

– удобство применения программных средств — оценка времени работы лица, ответственного за выполнение задачи, необходимого для выполнения расчетов (моделирования), удобство интерфейса и информативность отчетных материалов;

– адекватность выполняемых расчетов и математического моделирования с использованием программных средств — суммируемая количественная оценка, отражающая точность расчетов, а также корректность учета различных факторов при их выполнении и эффективность использования исходных данных;

– необходимое время на подготовку исходных данных.

Результаты работы с предприятиями промышленности позволили сформировать представление о текущей ситуации в области создания специального программного обеспечения, выявить наиболее перспективные образцы и выработать предложения по их использованию.

Ключевые слова: предприятия промышленности, поиск и отбор, специальное программное обеспечение, оценка, параметры, перспективные образцы, предложения по использованию.

ОСОБЕННОСТИ ОРГАНИЗАЦИИ УЧЕТА И ХРАНЕНИЯ ПРОГРАММНОЙ ПРОДУКЦИИ ВОЕННОГО НАЗНАЧЕНИЯ

Сковородкин Владимир Алексеевич

*27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, skovor@mail.ru*

Чеботков Кирилл Владимирович

*27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, zogel@mail.ru*

Скородулина Елена Юрьевна

*кандидат физико-математических наук,
27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, skorodulina@yandex.ru*

В последние годы, на фоне развития и внедрения новых информационных технологий, специалистами отмечаются высокие темпы разработки и, соответственно, стремительный рост числа программных продуктов различного предназначения, в том числе разрабатываемых в интересах Вооруженных Сил Российской Федерации. При этом без соответствующего контроля и координации разработок, проводимых по заказам различных органов военного управления, зачастую возникают предпосылки к многократному дублированию автоматизации процессов решения схожих наборов частных задач. Таким образом, актуальной становится задача систематизации накопленного научно-технического задела в области создания программной продукции, что в первую очередь предполагает организацию хранения всех имеющихся и вновь разрабатываемых программных средств с целью их дальнейшего использования.

В интересах решения указанной задачи проанализирован опыт создания и функционирования фондов и библиотек программной продукции различных федеральных органов исполнительной власти Российской Федерации. Особое внимание при этом уделено рассмотрению опыта организации работы Национального фонда алгоритма и программ, предназначенного для сбора, обработки и хранения созданной или приобретенной, с привлечением средств федерального бюджета программной продукции, а также для обеспечения к ней доступа государственных органов управления с целью дальнейшего использования в своей деятельности.

Вместе с тем рассмотрены основные этапы создания фонда алгоритмов и программ Министерства обороны Российской Федерации и его текущее состояние. Выявлены проблемные вопросы организационного и технического характера, возникшие при формировании фонда, наполнении его программной продукцией и предоставлении доступа к его ресурсам заинтересованным организациям. Приведены основные положения руководящих, методических и нормативно-справочных документов, регламентирующих организацию работы фонда, а также права и обязанности сторон, вовлеченных в эту работу.

На основе результатов проведенного анализа предложены основные ориентиры развития фонда алгоритмов и программ Министерства обороны Российской Федерации, которых стоит придерживаться в дальнейшем для его успешного функционирования в соответствии с целевым предназначением.

Ключевые слова: фонд алгоритмов и программ; программная продукция; учет и хранение программной продукции; научно-технический задел.

ПРИМЕНЕНИЕ МЕТОДОВ ФУНКЦИОНАЛЬНОГО ВЫБОРА ДЛЯ ОЦЕНИВАНИЯ СПЕЦИАЛЬНЫХ ПРОГРАММНЫХ СРЕДСТВ ВОЕННОГО НАЗНАЧЕНИЯ

Чеботков Кирилл Владимирович

*27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, zogel@mail.ru*

Дубровский Артём Анатольевич

*кандидат технических наук,
27 Центральный научно-исследовательский институт
Министерства обороны Российской Федерации,
г. Москва, Россия, muha-region67@yandex.ru*

За последние десятилетия в области автоматизации деятельности должностных лиц органов военного управления различных уровней, связанной с планированием применения и управления войсками (силами), в частности, в области аналитической поддержки принятия ими решений, проведено большое количество научно-

исследовательских и опытно-конструкторских работ по созданию специальных программных средств для автоматизированных систем управления военного назначения, реализующих расчетные задачи и математические модели различных объектов и процессов. В результате этих работ в сфере автоматизации управления был получен значительный научно-технический задел, открывающий заинтересованным лицам возможность выбора программных средств, в наибольшей степени удовлетворяющих их потребностям. Однако ряд предварительных исследований показал, что возможностей используемого для этих целей метода экспертных оценок недостаточно для решения задач квалиметрии современных специальных программных средств. К настоящему времени назрела необходимость доработки существующего или разработки нового методического аппарата, позволяющего получать качественные оценки каждого программного средства без вовлечения экспертов непосредственно в процесс оценивания, учитывая при этом все ключевые особенности областей применения этих средств, определяемые экспертами.

На основе проведенного анализа исследовательских методик, используемых в области квалиметрии различных объектов, и исходя непосредственно из особенностей целевого предназначения разрабатываемого методического аппарата, поэтапно был обоснован подход к оцениванию специальных программных средств на основе методов функционального выбора. Группа методов функционального выбора была отобрана, как наиболее подходящая для применения в оценивании специальных программных средств военного назначения, в связи с тем, что для процесса оценивания таких средств свойственна необходимость учета большого числа показателей качества, зачастую несравнимых точными математическими методами.

Особенностью вычисления оценок программных средств с применением отобранных методов является необходимость предварительной пошаговой подготовки ряда исходных данных. На первом шаге программное средство должно быть отнесено к одному из предварительно сформированных подмножеств. Границы подмножеств задаются, исходя из областей применения программных средств, из уровней управления, на которых они могут применяться, и из детализации расчетов (моделирования). Кроме того, на этом шаге должны задаваться различные ограничения на использование программных средств, которые должны учитываться в процессе оценивания (временные, технические, информационные и т.д.). На втором шаге, в соответствии с подмножеством, к которому было отнесено оцениваемое программное средство, экспертами осуществляется выбор показателей (характеристик) оценивания и их группирование. На заключительном шаге осуществляется выбор шкал показателей (характеристик), задается их важность (веса), осуществляются выбор функций, отображающих их значения в абсолютную шкалу, и выбор вида обобщающей функции.

В процессе непосредственного получения количественных оценок программных средств, согласно предлагаемому подходу, методом экспертных оценок вычисляются весовые коэффициенты характеристик (групп характеристик), для чего используются матрицы их парных сравнений, а затем на их основе, в соответствии с вновь разработанным алгоритмом, вычисляются итоговые оценки программных средств.

В заключение отмечено, что при привлечении на этапах выбора характеристик (группы характеристик) оценивания специальных программных средств разработанный подход может стать полезным инструментом для многих специалистов и организаций, а получаемые с его помощью оценки могут быть использованы в качестве исходных данных в ряде задач, выходящих за границы, определенные на этапе

задания целей разработки самого подхода: классификация программных средств, хранящихся в видовых (родовых) и центральных фондах алгоритмов и программ; поиск в фондах алгоритмов и программ программных средств, наиболее подходящих для решения задаваемых задач; сравнение нескольких программных средств между собой в целях определения наиболее удовлетворяющего заданным требованиям.

Ключевые слова: оценка программных средств; программные средства моделирования; метод экспертных оценок; научно-технический задел.

ПОСТРОЕНИЕ ПРОГНОЗА СИГНАЛОВ В АСУ С ИСПОЛЬЗОВАНИЕМ МОДЕЛЕЙ АВТОРЕГРЕССИИ СКОЛЬЗЯЩЕГО СРЕДНЕГО

Тележкин Владимир Федорович
доктор технических наук, профессор,
Южно-Уральский государственный университет,
г. Челябинск, Россия, telezhkinvf@susu.ru

Рагозин Андрей Николаевич
кандидат технических наук, доцент,
Южно-Уральский государственный университет,
г. Челябинск, ragozinan@susu.ru.

Саидов Бехруз Бадридинович
Южно-Уральский государственный университет,
г. Челябинск, Россия;
Таджикский технический университет имени М.С. Осими,
г. Душанбе, Таджикистан, matem.1994@mail.ru

В работе рассматривается прогнозирование сложных сигналов с использованием модели авторегрессии скользящего среднего. Задача использования математических моделей для описания поведения физических объектов широко распространена. Подобная задача не полностью определена, потому что в ней может участвовать ряд неизвестных факторов. Во многих задачах мы должны исследовать зависящие от времени динамические объекты. Для таких объектов невозможно предложить детерминированную модель, которая позволяет точно определить будущее поведение объекта. Тем не менее, мы можем предложить модель, которая позволит нам рассчитать вероятность того, что какое-то будущее значение будет лежать в определенном интервале. Такая модель называется вероятностной или стохастической. Модели временных рядов, необходимые для получения оптимального прогнозирования и регулирования, на самом деле являются стохастическими. В будущем необходимо

различать вероятностную модель или (как ее иногда называют) случайный процесс в виде реализации наблюдаемого временного ряда. Важным классом стохастических моделей для описания временных рядов, который привлекает больше внимания, являются так называемые стационарные модели. Они основаны на предположении, что процесс остается в равновесии относительно постоянного среднего уровня. Однако многие временные ряды часто лучше описывать как нестационарные и, в частности, как не имеющие естественного среднего значения. Широкий класс нестационарных процессов, называемых процессами авторегрессии - скользящего среднего предоставляет множество как стационарных, так и нестационарных моделей, которые адекватно описывают многие временные ряды, встречающиеся на практике. В исследовании, при формировании прогноза сигнала предлагается предварительная разбивка на полосные составляющие. С использованием быстрого преобразования Фурье и разделения спектра сигнала на восемь равных частотных компонент получены отдельные прогнозы каждой компоненты. Сумма этих сигналов (компонент) позволяет сформировать общий прогноз сигнала. Из полученных данных можно сделать вывод, что с увеличением количества прогнозируемых выборок (полосных компонент) исследуемого сигнала, прогноз становится более надежным, и в результате суммирования индивидуальных прогнозов более простых компонент, на которые разлагается исходный сложный сигнал, можно было получить более точные прогнозы сигналов. Метод разложения исходного ряда данных на более простые ряды (компоненты) с использованием преобразования Фурье показывает его эффективность при построении прогнозов сложных сигналов с использованием хорошо известного метода. Целью данной работы является постановка задачи прогнозирования сигналов различной степени сложности с применением модели авторегрессии-скользящего среднего и разработана методика получения достоверных прогнозов для сложных, быстро меняющихся сигналов.

Ключевые слова: прогнозирование сигналов; стохастическая модель; преобразования Фурье.

РАНГОВЫЙ АЛГОРИТМ СЕЛЕКЦИИ РЕЖИМОВ РАДИОИЗЛУЧЕНИЯ

Моисеев Александр Александрович

кандидат технических наук,
Научно-производственное предприятие «Технос–РМ»,
г. Мытищи МО, Россия, slow.coach@yandex.ru

Рассматривается алгоритм селекции режимов радиоизлучения, способный обеспечить решение этой задачи в условиях разнородности источников и сложной помеховой обстановки. Входом алгоритма является результат первичной обработки информации, в ходе которой оценивается длительность импульсов излучения, дина-

мика его частоты и амплитуды, а также их разброс. На базе этих величин формируются исходные решающие статистики — база наблюдаемого сигнала и вариации его частоты и амплитуды. Производные статистики формируются на основе исходных путем использования медианно – рекурсивного или максимально — рекурсивного сглаживания. Каждая из решающих статистик в рамках многопороговой процедуры, трансформируется в строку рангов, размер которой соответствует числу распознаваемых режимов. В совокупности эти строки образуют таблицу (матрицу) ранжирования, каждый из столбцов которой представляет собой дискретное описание опознаваемого режима. Текущая обработка наблюдения при этом состоит в формировании рангов для используемых решающих статистик, а опознание режима осуществляется либо в строгом соответствии со столбцами таблицы ранжирования, либо с использованием дополнительной процедуры голосования «2 из 3х». При этом проведенное рассмотрение показало, что использование этой процедуры может приводить к ложному опознанию и его применение не всегда целесообразно.

Пороги в составе многопороговой процедуры формируются как правило апостериорно на основе обработки соответствующих статистических данных. Проведенное рассмотрение показало, что изрезанность исходных статистик вызывает значительные ошибки в опознании и побуждает использовать сглаженные производные. Выяснилось, что предпочтительной производной статистикой является результат максимально — рекурсивной фильтрации исходной. Эта фильтрация представляет собой сочетание выбора максимального значения в скользящем окне и последующей рекурсивной фильтрации первого порядка. Проведенный численный эксперимент показал, что при этом обеспечивалась практически безошибочная селекция наблюдаемых режимов. Дополнительным преимуществом такой фильтрации является большая простота реализации поиска максимума в скользящем окне в сравнении с выбором медианы. В перспективе это обеспечивает повышенное быстродействие алгоритма.

Ключевые слова: селекция, ИРИ, помеховая обстановка, решающая статистика, скользящее окно, рекурсивная фильтрация, многопороговая процедура, ранг, таблица ранжирования, голосование «2 из 3х»

СПОСОБ ОЦЕНКИ ХАРАКТЕРИСТИК ОПТИКО-ТЕЛЕВИЗИОННЫХ КАНАЛОВ В УСЛОВИЯХ ПОМЕХ

Фролов Дмитрий Валерьевич

кандидат технических наук,
Военно-космическая академия имени А.Ф.Можайского,
г. Санкт-Петербург, Россия

Результаты астрономических наблюдений с помощью оптических телескопов традиционно осуществляется в условиях наблюдения, обеспечивающих уровень фонового излучения, равный фону ночного безоблачного неба. При этом в качестве ха-

рактеристики чувствительности приёмных телевизионных каналов, сопряжённых с оптическими телескопами, применяется величина, называемая проницающей способностью. Она характеризует минимально возможный блеск наблюдаемого источника излучения, выраженный в звёздных величинах, который ещё может быть обнаружен с требуемыми характеристиками обнаружения в процессе первичной обработки сигнала, наблюдаемого на уровне помехи, соизмеримой с фоном ночного безоблачного неба. При наблюдении за космическим объектом через слой земной атмосферы в телесном угле, ограниченном полем зрения оптико-электронного средства, на фоточувствительной поверхности создается равномерная освещённость, пропорциональная мощности помехи. «Изображение» космического объекта, формируемое оптической системой, соизмеримо с размером элемента разложения фоточувствительной поверхности. Для обнаружения сигнала, отраженного от космического объекта, оценку потока следует проводить на элементе разложения телевизионного растра. Однако блеск источника излучения не определяет величину проницающей способности приемных телевизионных каналов оптических телескопов. Он лишь создаёт световой поток, который, в зависимости от яркости источника и условий наблюдения, с определённой долей вероятности приёмным каналом может быть зафиксирован. Следовательно необходимо определять значение порогового сигнала при заданных вероятностях ложной тревоги и правильного обнаружения. Определив величину порогового сигнала, поставим в соответствие этой величине уровень освещённости апертурной плоскости, световой поток которой, пройдя все элементы оптического канала, создаст на выходе фотоприемника сигнал, равный пороговому сигналу. Другими словами — это пороговый сигнал, пересчитанный на вход оптической системы, является минимальной величиной освещённости апертурной плоскости входного зрачка оптической системы, определяющий предельно минимальную величину блеска, которая ещё может быть обнаружена приёмным каналом оптико-электронной станции с требуемым качеством. Целью данной работы является возможность обосновать требования к параметрам приёмных телевизионных каналов и обеспечить их реализацию в приёмных каналах оптических телескопов, предназначенных для проведения астрономических наблюдений в различное время суток.

Ключевые слова: оптические телескопы; приемные телевизионные каналы; условия наблюдения; проницающая способность; световой поток, астрономические наблюдения.

СПОСОБ ФОРМИРОВАНИЯ АДАПТИВНОГО СЦЕНАРИЯ ДИАЛОГА

Зюзин Алексей Владимирович

доктор технических наук, профессор,
Ярославское высшее военное училище противовоздушной обороны,
г. Ярославль, Россия, aleksey.zyuzin@mail.ru

Курчидис Виктор Александрович

доктор технических наук, профессор,
Ярославское высшее военное училище противовоздушной обороны,
г. Ярославль, Россия, idahmer2@yandex.ru

Морозов Павел Андреевич

кандидат технических наук, доцент,
Ярославское высшее военное училище противовоздушной обороны,
г. Ярославль, Россия, mpa24@mail.ru

Аношин Роман Игоревич

Ярославское высшее военное училище противовоздушной обороны,
г. Ярославль, Россия, idahmer2@yandex.ru

Проведенный анализ показывает, что в период непосредственной угрозы агрессии и, особенно в военное время возникает необходимость повышения эффективности управления войсками, за счет сокращения работного времени боевого расчета органа управления при решение полиадических задач управления. Одним из наиболее предпочтительных направлений сокращения работного времени боевого расчета органа управления является применение диалогового режима взаимодействия между лицами боевого расчета и автоматизированным рабочим местом комплекса средств автоматизации на основе применения запросов на естественно-подобном языке. Одним из элементов необходимым для организации такого взаимодействия, позволяющим учесть последовательность шагов диалога в зависимости от потребностей лиц боевого расчета является адаптивный сценарий диалога. Структура диалога при этом представляется в виде множества взвешенных ориентированных графов диалога. Такая формализация позволяет учитывать последовательность ввода данных при решении задач управления за счет выделения компонент сильной связности и определения порядка шагов диалога внутри них на основе отношений межфреймовых связей.

С целью учета изменений, вносимых в структуру взвешенного ориентированного директивного графа диалога в зависимости от поступившего запроса на естественно-подобном языке в запросе лиц боевого расчета выделяются его структурные составляющие: команда и множество условий. Множество условий после предикатно-предметной интерпретации и проверки на корректность значения представляются в виде пустого графа. Операция вычитания между взвешенным ориентированным директивным графом диалога и пустым графом позволяет сформировать множество результирующих шагов диалога и определить функцию перехода между ними. Расстановка шагов диалога по возрастанию приоритета, определенного на основе взвешенном ориентированном директивном графе, формирует адаптивный сценарий диалога.

Ключевые слова: оперативность управления; задачи управления; естественно-языковое взаимодействие; продукционно-фреймовая модель; шаг диалога; граф диалога.

СИСТЕМОТЕХНИЧЕСКИЕ РЕШЕНИЯ И ПРОГРАММНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА АСУ ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННОЙ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЙ СИСТЕМЫ

Раков Игорь Васильевич

кандидат технических наук,
публичное акционерное общество «Информационные телекоммуникационные технологии»,
г. Санкт-Петербург, Россия, i.rakov@inteltech.ru

Титов Григорий Сергеевич

публичное акционерное общество «Информационные телекоммуникационные технологии»,
г. Санкт-Петербург, Россия, g.titov@inteltech.ru

Автоматизированные системы управления (АСУ) территориально-распределенной организационно-технической системой широко применяются для поддержки принятия решений должностных лиц органов государственной власти федерального, регионального, муниципального уровней, а также в крупных государственных промышленных компаниях. Помимо функциональных требований, к современным АСУ данного класса предъявляются требования по обеспечению единого информационного пространства. Данные требования накладывают на программное обеспечение дополнительные условия — согласованности графического интерфейса пользователя, унификации формата обмена данными между программами, единой среды взаимодействия.

В работе предлагаются системотехнические решения по обеспечению единого информационного пространства АСУ рассматриваемого типа, в рамках которого осуществляется решение основных классов задач поддержки деятельности должностных лиц: определение регламента деятельности, планирование деятельности, исполнение, сбор и анализ данных обстановки.

В связи с особенностями территориально-распределенных организационно-технических систем, как объекта управления, ключевым фактором, влияющим на решение задач должностных лиц, является эффективность взаимодействия объектов и субъектов доступа. Рассматривается два основных вида взаимодействия: локальное и распределенное, для описания которых предлагаются модели организации программного обеспечения «процесс–ресурс» и «процесс-процесс» соответственно.

В соответствии с моделью «процесс–ресурс» предлагается классификация объектов единого информационного пространства как информационных ресурсов и информационных процессов: распределенные базы данных, рабочие бизнес-процессы, электронные документы и цифровые карты. Структура соответствующего программного обеспечения определяется исходя из параметров модели, которые можно определить по результатам решения оптимизационной задачи. В качестве примера предлагается оптимизационный критерий эффективности выполнения процессов на выбранной структуре ресурсов.

Модель «процесс–процесс» отражает особенности взаимодействия с учетом факторов сетевого взаимодействия. Современные программные технологии включают алгоритмы обеспечения взаимодействия с различными параметрами и качеством обслуживания. В статье предлагается типовая классификация требований к параметрам взаимодействия в АСУ рассматриваемого типа, предъявляемых основными классами задач поддержки деятельности должностных лиц.

Определение необходимых ресурсов подсистемы взаимодействия, обеспечивающих требуемые значения параметров взаимодействия, традиционно осуществляется индивидуально для конкретной АСУ. В статье предлагается подход к описанию ключевых зависимостей между параметрами взаимодействия и необходимыми ресурсами подсистемы взаимодействия на основе теории систем массового обслуживания. На примере трех основных переменных: величины буфера сообщений, пропускной способности канала связи, интенсивности потока сообщений, демонстрируется возможность определения параметров подсистемы взаимодействия как решения оптимизационной задачи.

Предложенная в статье классификация моделей взаимодействия компонентов программного обеспечения позволяет подобрать подходящие стандартизованные программные технологии и платформы: как существующие, так и перспективные.

Модель взаимодействия «процесс-ресурс» традиционно поддерживается такими программными технологиями, как реляционные СУБД, REST-сервисы, средства файловой системы, реализующими стандартную схему доступа «Объект»–«Валидатор доступа»–«Субъект». Данная схема непригодна для построения единого информационного пространства, т.к. в ней нет единого способа согласования разнородных информационных объектов и процессов. Предлагается использовать расширенную схему доступа, предполагающую дополнительный элемент — классификатор объектов, который содержит описание метаданных параметров взаимодействия. Перечень и состав параметров классификатора определяются системными свойствами информационного пространства: структурой и взаимосвязями между информационными объектами и процессами. В статье приводится описание перспективных программных технологий, которые могут быть использованы как элементы расширенной схемы доступа: технология ведения общесистемных словарей и справочников, редакторы шаблонов экранных форм и отчетов, системы ведения пользовательских баз данных.

Проведен анализ видов взаимодействия типа «процесс–процесс», требуемых в АСУ территориально-распределенных организационно-технических систем, на основании которого предложена подходящая программная технология. В основе предлагаемой технологии лежит стандартизованная схема взаимодействия «Издатель–Подписчик», допускающая возможность реализации различных дисциплин взаимодействия: точка–точка, точка–многоточка, с подтверждением и без подтверждения, с возможностью приоритизации потоков данных.

Ключевые слова: автоматизированная система управления; территориально-распределенная организационно-техническая система; единое информационное пространство; зона ответственности; информационный ресурс.

ФОРМИРОВАНИЕ ДЕСКРИПТИВНЫХ ДИАГНОСТИЧЕСКИХ ЗАПРОСОВ ПРИ ТЕХНИЧЕСКОМ ДИАГНОСТИРОВАНИИ РАДИОЭЛЕКТРОННОЙ АППАРАТУРЫ

Пушкин Константин Александрович

*Ярославское высшее военное училище противовоздушной обороны,
г. Ярославль, Россия, konstantinpush@gmail.com*

В процессе эксплуатации сложных технических комплексов обслуживающий персонал сталкивается с нештатными ситуациями, которые связаны с нарушением функционирования радиоэлектронной аппаратуры, входящей в состав этих комплексов. В основе этих нарушений лежат различные неисправности, обусловленные схемотехническими и конструктивными особенностями аппаратуры, а также особенностями режимов ее использования по назначению. Возникновение неисправностей радиоэлектронной аппаратуры связано с отклонением параметров от номинальных значений, что может быть выражено нарушением одного или нескольких свойств аппаратуры. Ключевую роль в восстановлении исправного состояния аппаратуры занимает операция диагностирования.

Для определения вероятного места и причины возникновения неисправности обслуживающему персоналу требуется выполнить ряд действий, направленных на получение диагностической информации. Информация такого вида содержит описание аппаратуры в виде набора свойств, характеризующих состояние или поведение аппаратуры, как не соответствующее нормативно-технической документации, то есть как неисправное. Во всяком таком свойстве может быть выделен один или несколько диагностических признаков, описывающих исправную или неисправную аппаратуры по одному из аспектов (структурный, функциональный, параметрический, и т.п.), благодаря чему обслуживающий персонал может составить «общую картину» возникшего в аппаратуре нарушения и ее связь с местом и причиной неисправности.

При диагностировании распространено использование диагностических моделей радиоэлектронной аппаратуры, известных как «диагностические портреты неисправностей», структура которых основывается на совокупности пар вида «признаки-причина». Диагностические портреты неисправностей радиоэлектронной аппаратуры, представленные подобным образом, в настоящее время приводятся в эксплуатационной документации на бумажных и электронных носителях преимущественно в текстовой или табличной форме на основе естественно-языковых средств и характеризуются низким уровнем формализации. Основным способом обращения обслуживающего персонала к этим моделям является применение не естественно-языковых средств, а запросных механизмов, основанных на использовании традиционных средств указания: ввод с клавиатуры, перемещение и нажатие кнопок мыши, выбор элементов меню и др. Это создает существенные ограничения в части оперативного формирования запросов к носителям эксплуатационной документации, а также получения диагностической информации в ответ на такие запросы, что приводит к нежелательным временным издержкам и негативно влияет на время выполнения операции диагностирования аппаратуры в целом.

С этой точки зрения в качестве одного из перспективных направлений повышения степени автоматизации процесса диагностирования следует отметить подход к представлению неисправностей в пространстве свойств, основанный на формализованной концептуализации предметной области. Этот подход позволяет выполнить

многоаспектное описание исправной и неисправной аппаратуры в предметных терминах и понятиях естественного языка, что обеспечивает единство формального и содержательного представления свойств аппаратуры. Целью данной работы является постановка задачи по формированию естественно-языковых запросов обслуживающего персонала к формализованной концептуальной диагностической модели аппаратуры.

Решение поставленной задачи связывается с выполнением анализа структуры запросов к формализованной концептуальной диагностической модели на естественном языке. Обращение обслуживающего персонала в форме запросов к автоматизированной системе диагностирования в целях определения вероятных мест и причин отказа означает наличие в запросах явного описания, как минимум, одного диагностического признака неисправности, который был выявлен или измерен на текущем этапе операции диагностирования.

На основе семантического анализа различных предложений запросов, содержащих описание свойств аппаратуры и/или признаков неисправностей, выделено 12 видов типовых шаблонов, которые в работе называются семантическими шаблонами. Эти шаблоны отличаются своей структурой и формальным представлением, так что их использование позволяет производить выделение базовых понятий и терминов в запросах и устанавливать смысловые связи между ними. Разновидность используемых языковых конструкций определяется многообразием диагностической информации, используемой в действиях обслуживающего персонала при диагностировании.

Разработанная грамматика с точки зрения построения систем поддержки принятия решений при техническом диагностировании выступает в качестве формализованной основы для формирования дескриптивных диагностических запросов на естественно-подобном языке. Это создает предпосылки для реализации голосовых интерфейсов в запросных механизмах систем поддержки принятия решения технического диагностирования, что обеспечивает повышение уровня автоматизации средств информационной поддержки обслуживающего персонала.

Новизна предложенного подхода состоит в том, что он основан на согласовании формализованной концептуальной диагностической модели радиоэлектронной аппаратуры и языковых средств формирования запросов, что позволяет в системах поддержки принятия решений технического диагностирования определять критерий выбора технического диагноза на естественно-подобном языке.

Ключевые слова: радиоэлектронная аппаратура; техническое диагностирование; диагностические модели; формализованная концептуализация; семантические шаблоны.

СЕКЦИЯ № 3

БЕЗОПАСНОСТЬ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВИТИЯ ТЕОРИИ И ПРАКТИКИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Смирнов Глеб Евгеньевич

*общество с ограниченной ответственностью «Корпорация «Интел групп»,
г. Санкт-Петербург, Россия, science.cybersec@yandex.ru*

В 2017 г. в России был принят федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Данный закон устанавливает перечень объектов и субъектов, относящихся к критической информационной инфраструктуре Российской Федерации, а также обязует специальные службы разработать комплекс мер направленных на обеспечение их информационной безопасности. В п. 8 ст. 2 данного федерального закона указан перечень сфер критической информационной инфраструктуры, в числе которых значится оборонная сфера и сфера связи.

Как показал анализ работ в области аудита информационных систем одним из наиболее важных, но при этом уязвимых для внешних воздействий объектов критической информационной инфраструктуры Российской Федерации являются телекоммуникационные системы специального назначения в составе единой сети электросвязи. Для анализа защищенности объектов критической информационной инфраструктуры в настоящее время создается Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак. Однако анализ перспективных технических решений по данной системе показывает недостаточную проработку практических вопросов контроля защищенности объектов критической информационной инфраструктуры. Анализ исследований в области стратегии развития комплекса Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак и систем управления информацией и событиями в безопасности (Security Information and Event Management) показывает отсутствие в этих системах подсистем какой-либо экспериментальной проверки защищённости контролируемых объектов.

Новым подходом оценки защищенности информационной безопасности объектов критической информационной инфраструктуры является аудит на основе экспериментальных исследований системы. Такой аудит, проводится с применением тестовых информационно-технических воздействий, соответствующих прогно-

зируемым воздействиям злоумышленника, с целью практической проверки эффективности технических или организационных мер защиты, а также выявления новых уязвимостей объекта критической информационной инфраструктуры. Основной формой проведения аудита информационной безопасности на основе экспериментальных исследований системы является тестирование объекта специальными информационно-техническими воздействиями. При этом в настоящее время научно-обоснованные требования к наборам информационно-технических воздействий, используемых при тестировании, не предъявляются. Таким образом, перспективным направлением исследования является повышение качества оценки защищенности объекта критической информационной инфраструктуры путем научно-обоснованного выбора тестовых информационно-технических воздействий для проведения его аудита.

В настоящее время, в большинстве случаев, аудит рассматривается как процесс проверки информационных систем на соответствие заранее определенным требованиям информационной безопасности. Вместе с тем, требования по информационной безопасности, как правило, формулируются по итогам анализа инцидентов, что приводит к тому, что они регулярно отстают от современных возможностей и практики действий нарушителей. Экспериментальное тестирование реальных информационных систем рассматривается исключительно как «тестирование на проникновение» или как «инструментальный аудит», при этом проведение такого типа аудита в отечественной практике не регламентируется каким-либо системным или хотя бы общетеоретическим подходом. В некоторых отечественных работах по тестированию на проникновение акцент делается на необходимости выявления наиболее «зрелищных» уязвимостей или тех уязвимостей устранение которых принесет максимальные экономические выгоды компании, выполняющий аудит. Анализ зарубежных и отечественных методик тестирования на проникновение показал, что они не содержат исчерпывающего обоснования параметров и критериев выбора тестовых информационно-технических воздействий, особенно применительно к объектам критической информационной инфраструктуры.

Вышеуказанные факторы позволили сформулировать проблемную ситуацию — между необходимостью повышения качества оценки защищенности объекта критической информационной инфраструктуры путем обоснованного выбора информационно-технических воздействий при проведении его аудита и невозможностью разработки такого научно-обоснованного решения, на основе современного уровня развития научно-методического аппарата аудита информационных систем в составе теории информационной безопасности.

Для разрешения данной проблемной ситуации может быть сформулирована актуальная цель исследования — повышения качества оценки защищенности объекта критической информационной инфраструктуры путем обоснованного выбора тестовых информационно-технических воздействий при проведении его аудита. Объектом исследования являются тестовые информационно-технические воздействия, используемые для оценки защищенности критической информационной инфраструктуры, а предметом исследования — качество набора тестовых информационно-технических воздействий, используемых для оценки защищенности объекта критической информационной инфраструктуры.

Для решения общей научной задачи в интересах достижения поставленной цели, она была декомпозирована на частные научные задачи:

1) разработка модели тестирования защищенности объекта критической информационной инфраструктуры;

2) разработка методики обоснования набора тестовых информационно-технических воздействий для оценки целевых уязвимостей объекта критической информационной инфраструктуры;

3) обоснования набора тестовых информационно-технических воздействий для рациональной полноты оценки уязвимостей объекта критической информационной инфраструктуры в условиях ограниченных ресурсов;

а также частную прикладную задачу:

4) разработка научно-обоснованных технических решений по архитектуре автоматизированного комплекса тестирования защищенности объекта критической информационной инфраструктуры.

Решением этих частных задач будут следующие научные и прикладные результаты значимые для развития теории аудита информационной безопасности и обладающие практическим эффектов в части повышения качества оценки защищенности объекта критической информационной инфраструктуры путем обоснованного выбора тестовых информационно-технических воздействий при проведении его аудита комплексом Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Ключевые слова: критическая информационная инфраструктура; информационная безопасность; Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак; аудит; тестирование; информационно-техническое воздействие.

АЛГОРИТМ УСТРАНЕНИЯ ПРОСКАЛЬЗЫВАНИЙ ЦИФРОВОГО СИГНАЛА С ИСПОЛЬЗОВАНИЕМ СВОЙСТВ СВЕРТОЧНЫХ КОДОВ

Синицын Юрий Юрьевич

Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
г. Краснодар, Россия, sinia90@mail.ru

Переладов Михаил Андреевич

филиал Военной академии материально-технического обеспечения (г. Омск)
г. Омск, Россия, perl@mail.ru

В цифровых системах передачи данных между источником информации и приемником информации возникает символьная синхронизации. При воздействии помех на передаваемое сообщение возможно изменение одного или группы символов, удаление или добавление лишних символов.

Для решения проблемы рассинхронизации цифровых системах используются устройства с эластичной памятью, в которых по тактовой частоте осуществляется запись переданного сигнала, по тактовой частоте генератора приемника происходит его считывание. Устройство с эластичной памятью используется для долгого хранения сигналов цифровой системы связи, эластично изменяясь для компенсации задержек во времени прохождения цифрового сигнала. Кратковременные отклонения

тактовой частоты компенсируются с помощью эластичной памяти. Данный вид памяти становится малоэффективным при наличии пусть и небольших, но продолжительных отклонений в синхронизации устройств. Это связано с тем, что такая память переполняется или опустошается в зависимости от соотношения тактовых частот. При этом возникает факт называемый проскальзыванием. Проскальзывание — это эффект, который получается при различиях в синхронизации приемной и передающей аппаратуры и, как следствие, ведет к пропуску информации или считыванию ее несколько раз подряд.

Для обнаружения и исправления ошибок, вызванных помехами в канале связи, используют корректирующие коды. Модификация алгоритма декодирования сверточных кодов по Витерби позволяет устранить не только искажения изменение одного или группы символов, но и искажения типа удаление или добавление лишних символов.

Анализируя процесс декодирования по Витерби, при нарастании значений метрик путей возможно определить место пропущенного (добавленного лишнего) бита информации. Вставка (удаление) бита с момента нарастания значения метрик путей позволит предотвратить распространение влияния эффекта проскальзывания кодовой последовательности цифрового сигнала.

Уменьшить влияние помех на сообщение, передаваемое по каналу связи возможно, используя свойства сверточных кодов. Модификация алгоритма декодирования по Витерби позволит восстанавливать символьную синхронизацию в цифровых системах передачи данных. Алгоритм представленный в данной статье возможно применять как для декодирования по алгоритму Витерби с жестким решением, так и для декодирования по алгоритму Витерби с мягким решением.

Ключевые слова: синхронизация цифрового сигнала; проскальзывания; сверточные коды; алгоритм декодирования по Витерби.

АУТЕНТИФИКАЦИЯ СЕАНСОВОГО КЛЮЧА НА ОСНОВЕ УНИВЕРСАЛЬНЫХ ХЭШ-ФУНКЦИЙ И СЛУЧАЙНЫХ ЦЕПОЧЕК БИТ

Яковлев Виктор Алексеевич

доктор технических наук, профессор,
Санкт-Петербургский Государственный университет телекоммуникаций
имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, viyak@bk.ru

Савинова Светлана Алексеевна

Санкт-Петербургский Государственный университет телекоммуникаций
имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, savinova-sveta@mail.ru

Исследуется способ аутентификации сеансовых ключей для мобильных устройств, формируемых методом Диффи-Хеллмана в условиях применения злоумышленником атаки «человек-посередине». Предполагается, что пользователи A и B, формирующие сеансовый ключ, имеют предварительно распределенные случайные цепочки бит $\boldsymbol{a}$ и $\boldsymbol{b}$ соответственно, полученные либо от некоторого источника,

либо сгенерированные ими самими на основе данных, полученных от магнитометров или акселерометров из состава мобильных устройств. Злоумышленник не имеет доступа к этим цепочкам. Особенность решения данной задачи состоит в том, что последовательности ***a*** и ***b*** в точности не совпадают. Предложен способ аутентификации значений Диффи-Хеллмана с использованием аутентифицирующих последовательностей ***a*** и ***b***. С этой целью сообщение (значение Диффи-Хеллмана) пользователем *A* разделяется на *N* блоков. Для каждого блока вычисляется аутентификатор с использованием универсального класса хеш-функций. Хэшфункция задается ключом, который выбирается как блок случайных цепочек ***a*** или ***b***. Значение Диффи-Хеллмана и аутентификаторы передаются по каналу пользователю B. На приемной стороне вычисляются аутентификаторы от принятого значения Диффи-Хеллмана, которые сравниваются с аутентификаторами принятыми из канала. Если число неправильно принятых аутенификаторов не превышает порог, установленный в системе аутентификация, то аутентификация значения Диффи-Хеллмана считается успешной. Нарушитель перехватывает значения Диффи-Хеллмана, аутентификаторы всех блоков и создает ложное сообщение (значение Диффи-Хеллмана). Рассматривается следующая стратегия действий нарушителя: там, где блоки в исходном и ложном сообщении совпадают, он использует перехваченные аутентификаторы; там, где блоки не совпадают, нарушитель формирует аутентификатор случайным образом. Предложен эффективный метод определения возможного отличия ложного сообщения от истинного в количестве блоков, учитывающий число отличающихся блоков и вероятность формирования такого сообщения. Получены соотношения для оценивания вероятности ложного отклонения ключа (из-за несовпадения цепочек ***a*** и ***b***) и вероятности навязывания ложного значения Диффи-Хеллмана. Приведен пример выбора параметров системы аутентификации ключа длиной 256 бит, обеспечивающей вероятностью навязывания ложного ключа не более 10–6 при вероятности ложного отклонения истинного ключа 10–6, что свидетельствует о реализуемости предлагаемого способа аутентификации.

Ключевые слова: аутентификация; распределение ключей; метод Диффи-Хеллмана; атака человек-посередине; универсальные хэш-функции.

АНАЛИЗ ЗАЩИЩЕННОСТИ БАЗ ДАННЫХ КАТАЛОГА ПРЕДМЕТОВ СНАБЖЕНИЯ ГРУПП ОДНОРОДНОЙ ПРОДУКЦИИ

Барильченко Семен Андреевич

*Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
г. Краснодар, Россия*

С развитием оборонно-промышленного комплекса и выходом на международный уровень потребовалась система классификации вооружения, военной и специальной техники (ВВСТ), обеспечивающая однозначную идентификацию продукции и ее составных частей. В результате появилась система каталогизации предметов снабжения групп однородной продукции.

Каталогизация применяется на всех этапах жизненного цикла ВВСТ от разработки до утилизации, для оптимизации номенклатуры ВВСТ, улучшения качества закупаемой продукции, выявления взаимозаменяемой и устаревшей продукции, повышения мобилизационной готовности экономики в интересах обороны и безопасности государства.

Каталог продукции для федеральных и государственных нужд представляет собой справочник для создания базы данных номенклатуры ВВСТ и другого имущества. Потеря указанной информации может привести к значительному экономическому ущербу, а также разглашению защищаемых государством сведений.

Из широкого спектра представленных баз данных структура каталога имеет ряд особенностей по построению содержимого и требованиям к защите информации.

Из трех основных свойств безопасности информации конфиденциальность, доступность, целостность вызывают интерес последние две. Для достижения целей противодействия реализации угроз информационной безопасности средства криптографической защиты информации (СКЗИ) являются наиболее надежными. Современные СКЗИ в базах данных успешно справляются с внешними воздействиями на систему безопасности, но защита от инсайдера остается на недостаточно высоком уровне.

По результатам ежегодного исследования утечек информации ограниченного доступа установлено, что на утечки, спровоцированные внутренним нарушителем, пришлось 9,8 млрд записей, что составляет 67,5% от совокупного количества записей, скомпрометированных в 2019 году.

Учитывая изложенное, полагается целесообразным разработать специальный метод защиты имеющейся базы данных каталогизации предметов снабжения номенклатуры групп однородной продукции от вмешательства внутреннего нарушителя.

Объектом исследования является база данных каталогизации групп однородной продукции номенклатуры средств защиты информации.

Предмет исследования — способ обеспечения целостности и доступности информации базы данных системы каталогизации номенклатуры средств защиты информации при воздействии внутренним нарушителем.

Авторами получено инновационное изобретение (патент Российской Федерации № 2726930). Заявка опубликована 10.12.2019. Патент опубликован 16.07.2020. Название изобретения: «Способ криптографического и рекурсивного 2-D контроля целостности метаданных файлов электронных документов».

Результатом исследования станет создание защищенной базы данных каталогизации групп однородной продукции номенклатуры средств защиты информации, в том числе для обработки сведений ограниченного распространения.

Ключевые слова: система классификации вооружения; оптимизация номенклатуры; утечка информации.

АНАЛИЗ ПУТЕЙ ОЦЕНКИ СОСТОЯНИЯ УРОВНЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В УЧРЕЖДЕНИИ

Селиверстов Александр Сергеевич

*Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
г. Краснодар, Россия, as.seliverstov93@gmail.com*

Оценка защищенности конфиденциальной информации в учреждении задача, требующая:

1) построения гибких многоуровневых моделей информационных систем, учитывающих не только программные и аппаратные ресурсы, но и организационные процессы документооборота;

2) разработки эффективных математических алгоритмов оценки текущего состояния информационной безопасности и прогнозирования возможных инцидентов информационной безопасности;

3) разработки методики оценки эффективности и прогнозирования системы информационной безопасности.

Современные методы оценки защищенности информации, предложенные в нормативно правовых актах Российской Федерации в области защиты информации, основаны на следующих принципах:

1) вводится иерархия классов безопасности, каждому классу соответствуют определенные требования к системе защиты информации;

2) соответствие системы информационной безопасности определенному классу показывает текущему состояние защищенности информационной системы в зависимости от её значимости, объема и ценности информации обрабатываемой в ней;

3) сравниваются возможные угрозы с текущем состоянием информационной безопасности, если система защиты закрывает угрозы, то применения дополнительных мер защиты не требуется.

Указанные особенности оценки защищенности информации не позволяют в полной мере спрогнозировать возможные каналы утечки информации, особенно в тех информационных системах, которые не подходят под классификации.

Альтернативным вариантом оценки защищенности конфиденциальной информации может быть логико — вероятностный метод расчета надежности, предложенный профессором Рябининым И.А.

Логико — вероятностный метод основан на применении алгебры-логики и теории вероятностей и позволяет решить следующие задачи в рамках защиты информации:

1) выявить объективно слабые места в системы защиты информации и причины возникновения опасных ситуаций;

2) определить оптимальную стратегию развития системы защиты информации;

Для оценки защищенности конфиденциальной информации с использование логико вероятностного подхода необходимо провести анализ учреждения, в результате которого:

1) с заданной точностью определить сущность опасного состояния, в качестве опасного состояния могут рассматриваться события утраты, разглашения, модификации, отказа доступа к информации;

2) определить границы исследуемого объекта;

3) определить возможные ситуации при составлении сценариев развития событий.

Для наиболее точных результатов анализа состояния защиты информации и прогнозирования опасных состояний необходимо решить задачу по вычислению наиболее приближенных к реальным условиям показателей вероятности наступления опасных ситуаций.

Ключевые слова: защита информации; информационная безопасность; оценка состояния защиты информации; логико-вероятностный метод; анализ защиты информации учреждения.

АНАЛИЗ ТРЕБОВАНИЙ К КАЧЕСТВУ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ, ИСПОЛЬЗУЕМЫХ ДЛЯ ПОДТВЕРЖДЕНИЯ ПОДЛИННОСТИ ПЕРЕДАВАЕМЫХ ФАЙЛОВ

Антонов Алексей Александрович

Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, г. Краснодар, Россия

Цифровой водяной знак (ЦВЗ) представляет собой дополнительную информацию, внедряемую в исходных файл с целью подтверждения подлинности источника. Кроме того ЦВЗ могут быть использованы для получения цифровых «отпечатков» (разные абоненты получают копии, помеченные разными водяными знаками), отслеживание трансляций (благодаря чему возможно отследить источник принятого файла) и сокрытие факта передачи информации. ЦВЗ используемые для защиты медиафайлов чаще всего невидимы, что позволяет скрыть от нарушителя факт наличия встроенного маркера.

Так как ЦВЗ наносится непосредственно на защищаемый файл то при передаче информации по каналу связи в результате деструктивного воздействия случайного или преднамеренного характера ЦВЗ так же, как и оригинальный файл может исказиться. Однако изменения передаваемого файла, из-за особенностей человеческого зрения, могут не сильно повлиять на качество восприятия, изменение же ЦВЗ приведет к потере доверия к источнику и нарушению связи. Соответственно, на этапе внедрения ЦВЗ необходимо оформить ряд требований к внедряемой информации, обеспечив ее помехоустойчивость с учетом особенностей передаваемой информации и условий внешней среды. На сегодняшний день в России отсутствуют нормативно-правовые акты, регламентирующие порядок использования ЦВЗ. Международные стандарты в зависимости от степени защиты от внешних воздействий классифицируют ЦВЗ на: хрупкие (применяются для защиты информации от изменений); полухрупкие (устойчивы к определенным типам атаки и не устойчивы к другим); робастные (обеспечивают защиты от большинства видов искажений).

Помехи в канале связи и активные действия злоумышленника могут привести к двум типам модификаций медиа информации: 1) шумоподобные (изменение значений

пикселей); 2) геометрические (пространственное изменение пикселей). Защита от шумоподобных помех обеспечивается введением избыточности в ЦВЗ. Защита от геометрических искажений обеспечивается применением различных алгоритмов внедрения ЦВЗ и так же введением избыточности.

Ключевые слова: цифровой водяной знак; сокрытие информации; избыточность; защиты информации; внедрение информации.

ВОПРОСЫ КИБЕРГИГИЕНЫ ПОЛЬЗОВАТЕЛЕЙ И ОПЕРАТОРОВ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ЭЛЕКТРОННОЙ БИБЛИОТЕКОЙ

Крюкова Елена Сергеевна
Военная академия связи имени Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия, e.kkrukovaa69@yandex.ru

Малофеев Валерий Александрович
Военная академия связи имени Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия, valeron12.1366@gmail.com

Паращук Игорь Борисович
доктор технических наук, профессор,
Военная академия связи имени Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия, shchuk@rambler.ru

В современном информационно-телекоммуникационном пространстве страны в целом, и информационной среде системы образования, в частности, все большую роль играют электронные (цифровые) библиотеки. Существуют различные подходы к определению, процедурам создания и совершенствования информационных систем типа «электронная библиотека», но основной постулат узаконен и остается неизменным – электронная библиотека представляет собой взаимоувязанную по целям и задачам, емкую и мощную информационную систему, предназначенную для организации и хранения упорядоченного фонда электронных объектов и обеспечения доступа к ним с помощью единых средств навигации и поиска. При этом важность электронных библиотек для сбора, хранения и снабжения информационными ресурсами легальных пользователей с помощью типовых программно-аппаратных средств, все время возрастает. Электронная библиотека способна оказать реальную помощь в информационном обеспечении, как в области подготовки и повышения квалификации профессиональных кадров, так и в области практической разработки технологий, технических систем, подсистем управления и автоматизации различных процессов в промышленности, финансовой сфере, обороне. Она способна обеспечить поиск

и управляемый доступ (по информационно-телекоммуникационным сетям) к электронным документам, базам данных, справочным и поисковым системам, а также к иным информационным ресурсам. Особая роль при этом возлагается на автоматизированную систему управления электронной библиотекой, которая имеет свои цели, состав и функции. К автоматизированной системе управления электронной библиотекой предъявляются современные требования, включая потребность в обеспечении кибербезопасности. Под кибербезопасностью понимается отрасль технических знаний, отвечающая за эффективное применение взаимоувязанной совокупности способов и средств поддержания устойчивой работы электронной библиотеки и автоматизированной системы управления электронной библиотекой в условиях целенаправленного деструктивного воздействия (в условиях киберугроз). Под киберугрозой понимается либо совокупность факторов и условий, создающих опасность нарушения кибербезопасности электронной библиотеки, либо угроза потери данных или нарушения ее работы в результате кибератаки – компьютерного (цифрового) несанкционированного воздействия на электронную библиотеку и/или автоматизированную систему управления ею специальными программными средствами с целью нарушения их работы, получения конфиденциальной информации или с иными негативными целями. Для предотвращения угроз кибербезопасности рассмотрена, поддержана и обоснована гипотеза о необходимости и практической целесообразности безусловного применения (в комплексе с традиционными средствами защиты) правил и процедур кибергигиены пользователей и операторов автоматизированной системы управления электронной библиотекой. Таким образом, актуальным предметом исследований может и должна быть современная кибергигиена, как набор практик кибербезопасности, совокупность методов и мер предосторожности, а также привычек, знаний и навыков защиты, которые позволяют существенно снизить риски киберугроз (последствий кибератак) для пользователей и операторов автоматизированной системы управления электронной библиотекой. Причем кибергигиена анализируется с системных позиций, как взаимосвязанный комплекс методов и практических шагов, которые пользователи и операторы автоматизированной системы управления электронной библиотекой на своих рабочих местах (устройствах) могут и должны предпринимать для поддержания работоспособности системы и повышения кибербезопасности. Кибергигиена способна решить ряд проблем, например: проблему некорректных (неверных) данных; проблему потери данных (не поддерживается резервное копирование); проблему устаревших приложений (программные приложения нуждаются в регулярном обновлении) и наконец, собственно проблему прямого нарушения кибербезопасности – перманентные и непосредственные киберугрозы (кибератаки, фишинг, хакеры и т.д.). Поэтому так важно детально проанализировать и заново, с учетом современных угроз, сформулировать частные задачи кибергигиены, наметить возможные пути их решения, направленные на создание актуальных и эффективных средств и методов поддержания киберустойчивости современных электронных библиотек и автоматизированных систем управления ими. С точки зрения практической значимости, представленный подход позволяет сформулировать и обосновать направления совершенствования качества и пути повышения эффективности кибергигиены, как многоуровневой и многоаспектной практики выполнения повседневных (иногда рутинных) операций по предотвращению киберугроз. Этот набор способов, методов и мер предосторожности, повторяющихся и обязательных к исполнению пользователями и операторами автоматизированных систем управления, при его внедрении в ежедневный процесс жизнедеятельности систем такого класса, позволит не только предотвратить серьезные последствия утраты или моди-

фикации собираемой, хранимой и обрабатываемой информации, но и осуществить прогнозирование рисков кибербезопасности электронных библиотек. Целью данной работы является анализ существующих и выработка новых направлений теоретических исследований и организационно-практических разработок в области кибергигиены пользователей и системных администраторов электронной библиотеки для обеспечения кибербезопасности как самой библиотеки, так и ее автоматизированной системы управления.

Ключевые слова: электронная библиотека; кибербезопасность; автоматизированная система управления; кибергигиена; ресурс; пользователь; оператор.

ИССЛЕДОВАНИЕ ПОДХОДОВ ДЛЯ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ БЕСПРОВОДНОЙ СЕТИ С ПРИМЕНЕНИЕМ РАЗЛИЧНЫХ LDAP РЕШЕНИЙ

Докшин Александр Денисович

Санкт-Петербургский государственный университет телекоммуникаций имени проф. М. А. Бонч-Бруевича,г. Санкт-Петербург, Россия, a.dokshin007@gmail.com

Ковцур Максим Михайлович

*кандидат технических наук, доцент,
Санкт-Петербургский государственный университет телекоммуникаций имени проф. М.А.Бонч-Бруевича, г. Санкт-Петербург, Россия, maxkovzur@mail.ru*

Прудников Сергей Владимирович

Санкт-Петербургский государственный университет телекоммуникаций имени проф. М.А.Бонч-Бруевича, г. Санкт-Петербург, Россия, prud2000@mail.ru

Таргонская Алина Игоревна

Санкт-Петербургский государственный университет телекоммуникаций имени проф. М. А. Бонч-Бруевича, г. Санкт-Петербург, Россия, targonskaya.ai@gmail.com

С каждым годом технология сетей WiFi становится все более распространенной и популярной. Среди населения WiFi уже является обыденной вещью, встречающейся почти на каждом шагу. WiFi — это технология беспроводной сети, основывающаяся на стандартах IEEE 802.11. Широкое распространение данная технология получила благодаря своей гибкостью и возможностью отказа от кабелей. Сегодня очень немногие организации внедряют проводные сети. Современные компании создают гибкие рабочие пространства, где сотрудники могут продуктивно работать независимо от определенного рабочего места. Беспроводное подключение к сети является ключевой частью этого процесса.

Несмотря на ряд преимуществ беспроводной сети WiFi, есть и обратная сторона. Поскольку сигнал также доступен за пределами здания, исходя из этого, есть возможность подключения к сети со стороны злоумышленников. Ноутбук, программные инструменты и возможные уязвимости — все, что нужно хакеру для проникновения в корпоративную WiFi сеть. Опираясь на возможные риски, ИТ-администраторы прини-

мают меры для защиты своих организаций. Один из способов добиться этого — подключить сеть WiFi к службе каталогов. Использование LDAP каждый пользователь сможет уникально войти в сеть. LDAP — специализированная база данных, предназначенная для хранения каталогов. Данные LDAP структурированы и иерархичны. LDAP определяется как стандарт для каталогов, которые являются службами, содержащими подробную информацию об учетных записях пользователей. Каталоги также могут содержать другие структурированные данные, но авторизации пользователей в беспроводной сети можно ограничиться главной функцией — это хранение учетных записей пользователей. Использование метода авторизации WiFi устройств с помощью LDAP отличается рядом преимуществ. Это и регулирование доступа пользователей средствами Active Directory, и более удобный способ входа в сеть. Для компаний, использующих технологии LDAP, аутентификация WiFi осуществляется через интеграцию с RADIUS-сервером. Сервер RADIUS выступает в качестве прокси-сервера для службы каталогов, обеспечивая безопасный вход для каждого пользователя. Таким образом, будет создана удобная и безопасная система подключения к WiFi сетям.

Ключевые слова: WiFi; LDAP; Active Directory; аутентификация; RADIUS.

К ВОПРОСУ О ПОНЯТИИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ СИСТЕМЫ УПРАВЛЕНИЯ

Лепешкин Олег Михайлович

доктор технических наук, доцент,
Военная академия связи имени Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия, lepechkin1@yandex.ru

Остроумов Олег Александрович

кандидат технических наук,
Военная академия связи имени Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия, oleg-26stav@mail.ru

Ковалев Дмитрий Сергеевич

Военная академия связи имени Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия, oleg-26stav@mail.ru

Каждый человек по статистике проводит порядка 6 часов в сети Интернет, переходя по различным web-страницам, общаясь в социальных сетях, скачивая файлы. В 21 веке пользователи используют миллиарды web-приложений, обеспечивающих выполнения множества функций. По причине их популярности и удобства они ежедневно подвергаются различным атакам со стороны нарушителей. Большинство web-приложений имеют низкий уровень защищенности. Поэтому использование Машинного обучения, в перспективе, может решить сразу две задачи - автоматизация процессов, которые ранее требовали участия человека и быстрая обработка, с последующим анализом огромных объемов информации и расчёт параметров, ис-

пользуя множество переменных. Для обеспечения информационной безопасности существуют различные механизмы и технологии. Классическое представление безопасного web-приложения представляет собой систему, включающую следующие аспекты – разграничение прав доступа, использования механизмов защиты баз данных от извлечения информации, постоянный поиск уязвимостей web-приложений, использование новых технологий обеспечения непрерывной работы сервера. С каждым днём Машинное обучение внедряют в больших масштабах в различные отросли информационных технологий - телекоммуникации, финансы, транспорт, производство и даже сельское хозяйство. На данный момент, обеспечение компьютерной безопасности является приоритетной задачей для всего мира. Использование машинного обучения позволит вводить новые потенциальные решения, независимо от сложности их реализации или затрате ресурсов, данный метод позволит автоматизировать любой процесс в любой области деятельности. Применение этой технологии в компьютерной и информационной безопасности, позволит обеспечить защиту и эффективную работу интернет ресурсов на основе которых, и совершенствуется технология Машинного обучения.

Одной из главных метрик эффективной работы умных сетей является критерий качества разработанной модели. При определении наиболее значимых параметров метода обучения, признаков и свойств модели необходимо формализовать критерий определения качества, на основе которого будет производится усовершенствование и оптимизация рассматриваемого процесса. Для этого можно использовать средний модуль ошибки оценки полученного прогноза, также может быть использована вероятность ошибки классификации. Для построения наиболее эффективной модели необходимо обеспечить наиболее точный выбранный критерий, на основе которого можно будет определить реальные потери или выигрыш на практике. Но анализировать среднее отклонение результатов прогнозирования и фактическими значениями необходимо на внешних данных, которые не были настроены для калибровки построенной модели, при этом не используя для сравнения обучающей выборки, в противном случае возможно появления проблемы переобучения. На каждом этапе обучения необходимо оценивать среднее качество результатов прогнозирования на предмет точности, чтобы обеспечить качественные итоговые результаты обучения. Использование кросс-валидации позволит обеспечить лучшие результаты, а именно оценку разброса в точности предсказания модели, также обеспечить проверку модели на предмет того, насколько статистически значимым является отличие точности одной модели от другой. При введении кросс-валидации в модель предсказания вся обучающая выборка делится на число случайных частей, из-за чего происходит искажения отдельных частей тренировочной выборки и отсутствие прежней структуры исходных данных. Для решения данной проблемы необходимо чтобы, все части обучающей выборки как можно более реалистично отражали всю полноту информации, поэтому случайное разбиение, как правило, необходимо производить стратифицировано, то есть сохраняя пропорции классов, а также сохраняя пропорций значений отдельных признаков во всех частях разбиения выборки. При оценке модели важно выбирать качественные признаки, доступные для измерения в момент прогнозирования, это позволит получить наиболее эффективную модель машинного обучения. Целью данной работы является разработка модели машинного обучения, обеспечивающая информационную безопасность web-приложения.

Ключевые слова: web-приложение; сервер; машинное обучение; аномально поведение; учетная запись; пользователь.

МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Миняев Андрей Анатольевич

*Санкт-Петербургский государственный университет телекоммуникаций
имени проф. М.А. Бонч-Бруевича,
г. Санкт-Петербург, Россия, minyaev.a@gmail.com*

Моделирование угроз безопасности информации в информационных системах является одним из основных этапов создания систем (подсистем) защиты информации информационных систем. С точки зрения законодательства Российской Федерации в области обеспечения безопасности информации этот этап жизненного цикла создания системы защиты информации является обязательным в соответствии с частью 2 статьи 19 закона №152-ФЗ «О персональных данных», в соответствии с пунктом 4 приказа ФСТЭК России от 18 февраля 2013г. №21, а также в соответствии с приказом ФСТЭК России от 11 февраля 2013г. №17: «определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации».

В соответствии с методическими документами регуляторов РФ этап моделирования угроз безопасности информации необходимо проводить на этапе создания системы защиты информации, т.е. в том случае, когда еще на создана системы защиты информации, а иногда и сама информационная система. В этом случае провести инструментальный анализ защищенности, необходимый в соответствии с методическими документами не представляется возможным. В этой связи моделирование угроз безопасности информации, как правило, проводится экспертным путем с привлечением специалистов в области информационной безопасности. Такой подход является трудоемким и не исключает известные недостатки экспертного метода.

В настоящее время в мире существуют множество методологий моделирования угроз безопасности информации. Основными их них являются следующие:

STRIDE and Associated Derivations.

PASTA (The Process for Attack Simulation and Threat Analysis).

LINDDUN (Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance).

CVSS (Common Vulnerability Scoring System).

Attack Trees.

Persona non Grata.

Security Cards.

hTMM.

Quantitative Threat Modeling Method.

Trike.

VAST Modeling.

OCTAVE.

Mitre.

БДУ ФСТЭК России.

По результатам проведенного исследования можно сказать о том, что существующие методологии в большинстве своем имеют существенные недостатки, а именно: большой объем данных, отсутствие документации, отсутствие автоматизированных средств моделирования угроз безопасности информации, необходимость в высокой квалификации специалистов по информационной безопасности.

Для преставления набора данных для автоматизированной обработки и разработки программного обеспечения использовался язык программирования Python 3 и технологии Data Science.

В качестве объекта исследования была выбрана территориально-распределенная ИС, которая является информационной системой обработки персональных данных и государственной информационной системой одновременно.

Была решена задача подготовки данных для реализации метода моделирования УБИ. Проведен анализ известных зарубежных и российских баз данных и знаний угроз безопасности информации, проведен анализ моделей угроз ряда территориально-распределенных ИС. На основе проведенного анализа выявлены недостатки и преимущества существующих методологий. Установлены ключевые особенности архитектуры территориально-распределенных ИС, определены сложности при моделировании УБИ для таких ИС. Подготовлен набор данных для метода моделирования УБИ, проведены необходимые работы для автоматизированной обработки набора данных, связанные с конвертацией данных. Были проанализированы нечеткие нейронные сети ANFIS, алгоритмы их работы. Выбрана наилучшая, основанная на нечеткой системе вывода Сугено-Такаги-Канга. Проведены эксперименты, по результатам которых определены наилучшие параметры сети, позволяющие достичь минимальную ошибку обучения сети \, равную 0,014. Разработано программное обеспечение для реализации метода моделирования УБИ на языке программирования Python 3ю Полученные результаты можно использовать для определения актуальных УБИ для территориально-распределенных ИС. в качестве продолжения работы по данной тематике могут являться разработка метода определения актуального нарушителя безопасности информации, а также уменьшения ошибки обучения сети.

Ключевые слова: угрозы безопасности информации; территориально-распределенные информационные системы; методологии моделирования; Data Science; ANFIS.

МОДЕЛЬ КАНАЛА НЕСАНКЦИОНИРОВАННОГО ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ

Синюк Александр Демьянович

доктор технических наук, доцент,
Военная академия связи имени Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия, eentrop@rambler.ru

Остроумов Олег Александрович

кандидат технических наук,
Военная академия связи имени Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия, oleg-26stav@mail.ru

В современных информационных системах большие объемы информации хранятся в накопителях на жестких магнитных дисках. Удаление файлов средствами операционной системы или переформатирование магнитного накопителя не удаляет

данные. Удаление файлов штатными средствами операционной системы или переформатирование магнитных накопителей практически не удаляет данные. Это связано с тем, что при удалении файла с закрытой информацией штатными средствами операционной системы сама информация не перезаписывается. Драйвер отмечает, что соответствующая файловая запись не используется и, соответственно, сектора накопителя, содержавшие данные удаленного файла становятся свободными для записи новой информации. В условиях, когда данные файлов удаленные таким образом не будут перезаписаны существует возможность их восстановить и считать с накопителя.

Известен ряд методов уничтожения информации. Первая группа — это аппаратные методы, которые выводят носитель из строя путем его уничтожения. Применение аппаратных методов не всегда рационально и экономически оправдано.

Вторая группа методов - это программные методы, которые многократно перезаписывают сектора с удаленными данными псевдослучайной последовательностью и таким образом маскируют защищаемую информацию. Существенные недостатки программных методов заключаются в их низкой надежности и невысоком быстродействии. Проведенные исследования показали, что в ходе перезаписи поверх удаляемой информации, маскирующей последовательности символов, на крайних областях магнитных дорожек жесткого диска остаются поверхности некоторой намагниченности, содержащие информацию об удаленной записи. Нарушитель может провести исследование с помощью специальных устройств магнитный рельеф поверхности пластины жесткого диска для восстановления удаленных данных путем перезаписи другой информации.

Остается возможность их восстановления нарушителем в условиях перемещения накопителя из контролируемого помещения для утилизации, отправки в ремонт, воровства, замены, подмены, дарения и др.

Проводится селекция современных методов восстановления информации. В ходе реализации программных методов уничтожения информации выполняется перезапись сверху удаляемой информации маскирующей последовательности. Это не дает гарантии ее уничтожения, т.к. траектория движения записывающей головки жесткого диска не совпадает точно с магнитной дорожкой и по краям формируются области остаточной намагниченности, несущие информацию о предыдущих записях.

Предполагается, что нарушитель владеет одной из совершенных технологий восстановления информации с высоким разрешением исследования областей остаточной намагниченности. В ее качестве предложена технология магнитной сканирующей микроскопии, которая тесно связана с увеличением плотности записи информации на накопителях. Проведённый анализ принципов работы современных магнитных сканирующих микроскопов позволил создать условия для разработки модели канала несанкционированного восстановления информации, которая включает источник информации, представляющий собой поверхность накопителя, и оборудование нарушителя для доступа к остаточной информации. Источник с нарушителем связывает канал передачи информации, который предлагается описать моделью двоичного симметричного канала без памяти. Приводятся оценки вероятности ошибочного восстановления блока удаленной информации и среднего числа ошибок в информационном блоке.

В результате проведенных исследований с учетом адекватной оценки условий несанкционированного доступа нарушителя выбрана рациональная по критерию максимальной разрешающей способности современная технология доступа к удаленной (перезаписанной) информации на накопителях на жестких магнитных дис-

ках, которая называется магнитной сканирующей микроскопией. Использование ее нарушителем создает предпосылки для успешного несанкционированного доступа к защищаемой информации, подлежащей удалению с магнитных накопителей. Исследования технологии магнитной сканирующей микроскопией показали, что задача восстановления перезаписанной информации является достаточно сложной с отличной от нуля вероятностью ошибочного считывания (детектирования) конфиденциальных данных.

Разработана модель канала несанкционированного восстановления информации описывающая модель нарушителя, условия ведения условия несанкционированного доступа к критичной информации, модель канала считывания информации в рамках адекватных допущений и ограничений. Особенности процесса восстановления информации, выбранный минимально возможный размер блока данных, независимость его считывания и ненулевая вероятность ошибочного детектирования процедур технологии магнитной сканирующей микроскопией предопределили описание предлагаемого канала несанкционированного восстановления информации моделью двоичного симметричного канала без памяти.

Предлагаемая модель может быть рекомендована специалистам в области построения подсистем защиты информации от несанкционированного доступа современных информационных систем для синтеза адекватной модели нарушителя, разработки и селекции методов защиты, а также оценки надежности предлагаемых методов уничтожения конфиденциальной информации.

Ключевые слова: накопители на жестких магнитных дисках, удаление конфиденциальной информации, области остаточной намагниченности, нарушитель, магнитная силовая микроскопия, канал несанкционированного восстановления информации, модель двоичного симметричного канала без памяти.

МОДУЛЬ ПРИНЯТИЯ РЕШЕНИЙ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ СЕТИ

Евглевская Наталья Валерьевна

кандидат технических наук,
Военная академия связи имени маршала Советского Союза С.М.Буденного,
г. Санкт-Петербург, Россия, n.evglevskaya@gmail.com

Привалов Андрей Андреевич

доктор военных наук, профессор,
Петербургский государственный университет путей сообщения
Императора Александра I, г. Санкт-Петербург, Россия, aprivalov@inbox.ru

При создании информационной инфраструктуры автоматизированной системы управления на базе современных информационно-коммуникационных сетей возникает вопрос о защищенности этой инфраструктуры от угроз информационной безопасности.

Анализ защищенности автоматизированной системы управления от угроз безопасности информации - работа непростая. Умение оценивать и управлять рисками, знание типовых угроз и уязвимостей, владение методами анализа и специализированным инструментарием, знание различных программно-аппаратных платформ, используемых в современных информационно-коммуникационных сетях - вот далеко не полный перечень профессиональных качеств, которыми должны обладать специалисты, проводящие работы по анализу защищенности автоматизированных систем управления.

Анализ защищенности является основным элементом таких взаимно пересекающихся видов работ как аттестация, аудит и обследование безопасности автоматизированной системы управления. Таким образом обеспечение комплексного подхода к автоматизации деятельности, связанной с анализом защищенности объекта информатизации, является одной из ключевых задач информационной безопасности.

В настоящее время не существует каких-либо стандартизированных методик анализа защищенности автоматизированной системы управления, поэтому в конкретных ситуациях алгоритмы действий аудиторов могут существенно различаться. Однако типовую методику анализа защищенности объекта информатизации предложить все-таки можно. И хотя данная методика не претендует на всеобщность, ее эффективность многократно проверена на практике.

Для возможности проведения всеобъемлющего анализа угроз безопасности на основе строгих математических методов, позволяющих выявить и устранить критические уязвимости в системе защиты, разработан программный комплекс, реализующий автоматизированный анализ защищенности автоматизированной системы управления, исходя из параметров сетевой инфраструктуры объекта и элементов, входящих в её состав, а также возможностей нарушителя по реализации угроз. Задача анализа объекта декомпозируется на отдельные подзадачи, представляющие собой взаимосвязанные модули, каждый из которых определяет некоторый шаг анализа. Реализация каждого из модулей в виде совокупности согласованных функций обеспечивает унификацию программного комплекса и дает возможность адаптивной модификации в соответствии с актуальными требованиями безопасности для конкретного объекта информатизации.

Ключевые слова: нарушитель; автоматизированная система управления; информационно-коммуникационная сеть; угроза; информационная безопасность.

МОДЕЛЬ УСТОЙЧИВОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ

Билятдинов Камиль Закирович,
кандидат военных наук, доцент
акционерное общество «Центральный научно-исследовательский институт экономики, информатики и систем управления», г. Москва, Россия, k74b@mail.ru

Красов Андрей Владимирович,
кандидат технических наук, доцент,
Санкт-Петербургский государственный университет телекоммуникаций имени проф. М. А. Бонч-Бруевича, г. Санкт-Петербург, Россия, krasov@inbox.ru

Меняйло Вера Владимировна,
кандидат филологических наук,
Национальный исследовательский университет «Высшая школа экономики», г. Санкт-Петербург, Россия, menyaylo917@mail.ru

В настоящее время необходимым условием безопасного и эффективного функционирования автоматизированных систем управления различного назначения (далее – АСУ) является их устойчивость. В классическом понимании устойчивость – это свойство системы восстанавливать состояние равновесия, из которого она была выведена под влиянием возмущающих факторов после прекращения их воздействия.

Однако, анализ современных зарубежных научных исследований в сфере обеспечения безопасности, эффективности и устойчивости АСУ показывает ярко выраженную тенденцию расширения взглядов на устойчивое функционирование АСУ в неблагоприятных условиях. В первую очередь, это выражается в запросах на моделирование состояний устойчивости систем в зависимости от последствий деструктивных воздействий и с учетом качества программных систем и других обеспечивающих элементов в составе АСУ. Вышеизложенное обосновывает следующую постановку задачи: разработать простую и универсальную модель устойчивости АСУ для решения задач моделирования состояний устойчивости АСУ различного назначения в зависимости от последствий деструктивных воздействий на АСУ, качества программных систем и других элементов в составе АСУ (далее – Модель). Разработанная Модель представляет собой математическое описание состояний устойчивости объекта на основе критериев устойчивости и возможностей АСУ к восстановлению. Назначение Модели: анализ и оценка устойчивости систем, прогнозирование состояния АСУ в зависимости от последствий воздействия различных неблагоприятных факторов и сокращение времени и ресурсов на принятие обоснованных управленческих решений. Модель позволяет учитывать изменение исходных показателей функционирования систем в зависимости от результатов воздействия неблагоприятных условий. Для этого Модель включает в себя совокупность взаимосвязанных таблиц, содержащих описание требований, критериев и динамику изменений следующих основных показателей: время устойчивого функционирования, ресурсы, количество подсистем (элементов), количество персонала, трудозатраты, неисправности, возможности системы к восстановлению и результаты восстановления. В разработанной Модели описание состояния устойчивости объекта АСУ в любой момент времени происходит с помощью систематизированных значений выбранных показателей качества функционирования АСУ с последующей оценкой значений этих показателей в соответствии с заданными

критериями. В Модели основная величина, характеризующая влияние качества систем на устойчивость АСУ, – это количество времени, в течение которого АСУ способна устойчиво функционировать в неблагоприятных условиях без поступления внешних ресурсов и при одинаковом количестве ресурсов, имевшихся у АСУ в исходном состоянии, то есть до начала воздействия неблагоприятных условий. Таким образом, время устойчивого функционирования можно обоснованно считать основным показателем качества при оценке (сравнении) различных систем в сфере устойчивости аналогичных АСУ, функционирующих в одинаковых неблагоприятных условиях, или, например, при оценке качества АСУ до и после модернизации. Критерий оценки устойчивости АСУ состоит в том, что объект АСУ устойчив, если в любой момент оцениваемого периода времени значение выбранного показателя качества больше или равно своему минимально допустимому значению. Критерий оценки возможностей АСУ по обеспечению своей устойчивости за счет восстановления неисправных (поврежденных) элементов: АСУ устойчива, если в любой момент оцениваемого периода времени значение, выражающее наличие запасов ресурсов и количества восстановленных элементов АСУ, больше или равно значению, которое выражает потери ресурсов и потери (неисправности) элементов АСУ. То есть для обеспечения своей постоянной устойчивости система должна вовремя восстанавливать свои потери, в соответствии с установленными требованиями. Поэтому на устойчивость влияет время восстановления систем – элементов АСУ, от которых зависит достижение цели функционирования. Минимальное количество времени на восстановление элементов в составе АСУ будет всегда равно минимально возможному времени восстановления одного элемента. В Модели состояние устойчивости объекта в любой момент времени описывается путем заполнения таблицы «Изменение состояния объекта и оценка его устойчивости в результате воздействия неблагоприятных условий на объект» (далее – таблица). Таблица заполняется на основании описания исходного состояния объекта в заданные моменты времени, а также информации о результатах воздействия неблагоприятных условий на АСУ. В таблице учитывается время воздействия на объект неблагоприятных условий (деструктивных воздействий), в результате которых объект АСУ несет какие-либо потери: персонала, элементов, ресурсов и (или) может не достичь минимально требуемого результата функционирования. Динамика изменений состояний устойчивости описывается в Модели путем построения таблицы с помощью установленных критериев и формул расчета. Модель применяется в программе для ЭВМ «Оценка устойчивости систем» (свидетельство о государственной регистрации программ для ЭВМ № 2020615328, дата государственной регистрации 21.05.2020 года). В заключении необходимо отметить, что результаты моделирования устойчивости АСУ рационально использовать при подготовке и обосновании управленческих решений, принимаемых в процессе эксплуатации АСУ, в части касающихся совершенствования эксплуатации и технического обеспечения, а также в вопросах подготовки персонала.

Ключевые слова: автоматизированные системы управления; программные системы; качество; устойчивость; модель; время; ресурсы.

ОБЕСПЕЧЕНИЕ ДОСТОВЕРНОСТИ ПЕРЕДАЧИ СПЕЦИАЛЬНОЙ ИНФОРМАЦИИ В КОМПЛЕКСАХ С БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ

Задвижкин Алексей Анатольевич

*Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
г. Краснодар, Россия, z2a82@yandex.ru*

В условиях широкого распространения комплексов с беспилотными летательными аппаратами, а также ростом их функциональных возможностей повышается интенсивность воздействия злоумышленников на информацию, обрабатываемую в комплексах с беспилотными летательными аппаратами. Данные факты обуславливают актуальность исследования в области защиты информации в данных комплексах. Одним из видов информации, обрабатываемой в комплексах с беспилотными летательными аппаратами является специальная информация – данные, получаемые оптико-электронной системой, чаще всего представляющие фотоизображения, дополненные данными необходимыми для их использования: координатами места съемки, углами позиционирования оптико-электронной системы, а также другими данными. На передаваемую по радиоканалу специальную информацию возможно воздействие непреднамеренных помех, а так же целенаправленных деструктивных воздействий со стороны злоумышленника. Деструктивным воздействиям подвергается обе составляющие специальной информации. Передача специальной информации с борта беспилотного летательного аппарата возможна как на наземный пункт управления, непосредственно выполняющий управление полетом беспилотного летательного аппарата, так и на мобильные пункты приема специальной информации, которые только получают данные с результатами наблюдения. В последнем случае наиболее важным является обеспечение достоверности информации, в частности ее целостности. Существующие механизмы контроля и обеспечения целостности специальной информации не учитывают структуру передаваемых данных и чаще всего заключаются в применении равномерного помехоустойчивого кодирования на канальном уровне взаимодействия, а также применение решающей обратной связи. Однако, при получении специальной информации мобильными пунктами приема и обработки отсутствует возможность использования обратной связи, а искажение различных частей передаваемых данных оказывает различное влияние на показатели качества полученной информации в целом. Для повышения достоверности передачи специальной информации предложен способ, отличающийся применением помехоустойчивого кода с повышенной исправляющей способностью к отдельным частям специальной информации на прикладном уровне взаимодействия с компенсированием вводимой избыточности за счет применения методов стеганографии. Целью работы является разработка способа повышения достоверности передачи специальной информации в комплексах с беспилотными летательными аппаратами с учетом ее структуры и показателей качества принятой информации на мобильных пунктах прима и обработки специальной информации.

Ключевые слова: беспилотные летательные аппараты; целостность; достоверность; помехоустойчивое кодирование; стеганография.

ОБНАРУЖЕНИЕ СТЕГОСИСТЕМ, ИСПОЛЬЗУЮЩИХ ПОГРУЖЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В КОНТУРЫ ИЗОБРАЖЕНИЯ

Коржик Валерий Иванович

доктор технических наук, профессор
Санкт-Петербургский государственный университет
телекоммуникаций имени проф. М. А. Бонч-Бруевича,
г. Санкт-Петербург, Россия, val_korzhik@yandex.ru

Нгуен Зуи Кыонг

Санкт-Петербургский государственный университет
телекоммуникаций имени проф. М. А. Бонч-Бруевича,
г. Санкт-Петербург, Россия, cuong0111@gmail.com

Даньшина Арина Викторовна

Санкт-Петербургского государственного университета
телекоммуникаций имени проф. М.А.Бонч-Бруевича,
г. Санкт-Петербург, Россия, arina_danshina1999@mail.ru

Общеизвестно, что использование стегосистем повышает информационную безопасность хранения и передачи конфиденциальной информации. Действительно, в отличие от криптографии, стегосистемы (СГ) обеспечивают скрытие не только содержания, но и самого факта присутствия конфиденциальных данных в «невинных» покрывающих объектах (ПО), важнейшими из которых являются, изображения, звуковые и текстовые файлы, интернет-протоколы. Помимо очевидного использования СГ государственными структурами, в последнее время такая технология используется и в бизнес сообществе для обеспечения организационной или технической конфиденциальности. С другой стороны, является актуальной и технология обнаружения СГ, поскольку это позволяет организациям и компаниям защитить конфиденциальную информацию от ее утечки во внешний контур. Наиболее популярными ПО для использования СГ являются неподвижные изображения (цветные или с градациями серого), поскольку их использование в качестве носителей скрытой информации, например, в электронной почте, выглядит наиболее естественным.

Практическая важность, рассмотренных задач в представленной статье, стимулирует интенсивную разработку СГ и методов их обнаружения при помощи стегоанализа (СГА). Рассматривается перспективная стегосистема с погружением конфиденциальной информации в контуры неподвижного изображения с градациями серого. Описывается метод нахождения контуров изображения и алгоритм погружения в них информации. Оценивается объем вложенной информации, а также возможности обнаружения вложения визуальным и гистограммным методами. В качестве более эффективного метода обнаружения предлагается использовать подход, основанный на тестах псевдослучайности. Приводятся результаты экспериментальных исследований, подтверждающие целесообразность использования предложенного метода обнаружения.

Ключевые слова: стегосистема; контуры изображения; тесты на псевдослучаность; метод опорных векторов.

ОПРЕДЕЛЕНИЕ ХАРАКТЕРИСТИК МОДУЛЕЙ СИСТЕМЫ ХРАНЕНИЯ ДАННЫХ О СОБЫТИЯХ И ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Королев Игорь Дмитриевич
доктор технических наук, профессор,
Краснодарское высшее военное училище имени генерала армии С.М.Штеменко,
г. Краснодар, Россия, pi_korolev@mail.ru

Литвинов Евгений Сергеевич
Краснодарское высшее военное училище имени генерала армии С.М.Штеменко,
г. Краснодар, Россия, litvinoves@rambler.ru

Активное внедрение и использование средств вычислительной техники, различных средств автоматизации и автоматизированных систем, средств хранения и автоматизированной обработки информации, а также активное использование ресурсов различных информационно-телекоммуникационных сетей является неотъемлемой составляющей инфраструктуры практически всех предприятий и организаций во всем мире. Информационный обмен с использованием этих средств может быть как внутренним, так и внешним. При этом, физическое расстояние между автоматизированными рабочими местами должностных лиц перестает играть значимую роль для инфраструктуры этих организаций. Так, сотрудники организаций могут осуществлять обмен информацией с использованием персональных компьютеров (как стационарных, так и мобильных) или смартфонов, а также получать удаленный доступ к своему стационарному автоматизированному рабочему месту, находясь практически в любой точке земного шара.

Реализация этих возможностей создает предпосылки для вмешательства нарушителя (внешнего и/или внутреннего), что ставит задачу об организации и проведении как технических, так и организационных мер по обеспечению доступности, целостности и конфиденциальности обрабатываемой информации.

Наиболее эффективным на сегодняшний день комплексом мероприятий для борьбы с нарушителями является внедрение политики информационной безопасности и ведение аудита и мониторинга состояния автоматизированных систем центрами информационной безопасности.

Для решения этой задачи используются:

– средства защиты информации, находящиеся непосредственно на средствах вычислительной техники пользователей и серверов;

– системные журналы;

– системы предотвращения утечки информации и др.

Основным инструментом при работе центров информационной безопасности является средство выявления и обработки инцидентов и событий информационной безопасности.

Обработка инцидентов и событий информационной безопасности подразумевает проведение ряда технических и организационных мероприятий, направленных на локализацию инцидента, его устранения и ликвидацию последствий инцидента.

Для успешного выполнения этих задач в локальной сети и на оконечных ее узлах принято производить установку и настройку собственной системы управления инцидентами информационной безопасности.

В настоящее время активно используются следующие системы управления инцидентами информационной безопасности:

MaxPatrol SIEM – производства компании «Positive Tecnology»;

ArchSide – производства компании «HP» и др.

Все эти системы позволяют хранить данные о событиях и инцидентах информационной безопасности в собственной базе данных. Данные о событиях и инцидентах информационной безопасности поступают в базу данных после прохождения процедуры сбора, фильтрации и нормализации.

Такая схема работы имеет несколько недостатков:

1. База данных подчиняется правилам хранения и обработки данных системы управления инцидентами информационной безопасности, что не дает возможности для внесения изменений в структуру хранения без внесения изменения в ее модули;

2. Единовременная работа системы по сбору данных, их нормализации, корреляции и визуализации создает неравномерную нагрузку и увеличивает время обработки запроса в базе данных, что в свою очередь увеличивает время получения ответа на запрос оператором;

3. Невозможность ведения политики резервирования базы данных в режиме реального времени;

4. Отсутствие модуля хранения ненормализованных данных делает невозможным оперативное получение дополнительной информации о произошедшем событии (инциденте);

5. Отсутствие модуля хранения данных о контролируемом узле делает невозможным оперативное получение данных о состоянии этого узла;

6. Замкнутость системы делает невозможным подключение дополнительных модулей, не входящих в состав системы;

7. Подчиненность модуля хранения данных системе не дает возможности ведения отдельной политики безопасности относительно хранимых в системе данных, и др.

Таким образом, изменение порядка хранения и представления (визуализации) данных позволит повысить такие характеристики всей системы обнаружения и обработки событий и инцидентов информационной безопасности, как оперативность, надежность и безопасность. Кроме того, это добавит возможность внесения изменений в структуру хранения данных и взаимодействия с новыми программными средствами, разрабатываемыми сторонними производителями.

Для решения этой задачи необходимо определить требования, которым должна соответствовать подсистема хранения данных о событиях инцидентах информационной безопасности.

Во-первых, расположение оборудования, входящего в состав подсистемы банка данных событий и инцидентов информационной безопасности, должно иметь минимально-возможный физический разнос;

Во-вторых, техническое и программное составляющие подсистемы должны формировать зону ответственности, затрагивающую интересы и возможности одного должностного лица (отдела);

В третьих, порядок работы подсистемы должен подразумевать внедрение определенной политики безопасности, режима доступа, ведения аудита и мониторинга состояния;

В четвертых, проведение технических работ по резервированию и техническому обслуживанию программной и аппаратной составляющей оборудования;

В пятых, возможность внедрения схемы хранения данных, снижающий уровень избыточности информации;

В шестых, подсистема хранения данных о событиях и инцидентах информационной безопасности должна давать возможность формирования исходных данных для аналитических систем (обладать интерфейсами взаимодействия на уровне программного обеспечения).

При этом, СУБД должна обладать большим набором модулей, способных формировать хранение данных в объектно-реляционном виде и способна проводить оперативную выгрузку данных в затребованном оператором виде. Кроме того, ее функциональные возможности должны обладать средствами гибкой настройки механизмов защиты хранимых данных и разграничения доступа к этим данным.

Однако, использование одной системы управления базами данных не является достаточным для решения остальных задач и требует внедрения дополнительных модулей.

Так как поток данных о выявленных событиях и инцидентах информационной безопасности предоставляется средствами, разрабатываемыми различными производителями, необходимо использовать модуль репликации данных, который будет агрегировать данные в одном месте с учетом возможностей и требований интерфейсов взаимодействия на уровне программного обеспечения этих средств.

Так как контролируемые средства вычислительной техники и коммутации могут находится на значительном отдалении от системы управления инцидентами информационной безопасности, или линии связи могут обладать низкой скоростью (или качеством) передачи данных, необходимо произвести уменьшение передаваемого трафика, без утраты его информативности, для чего необходимо использовать модуль кодирования/декодирования передаваемых данных с возможностью автоматического формирования словаря кодирования передаваемых данных.

Для предоставления пользователям возможности ознакомления с хранимой в подсистеме информации, необходимо также произвести разработку отдельного модуля визуализации данных о событиях и инцидентах информационной безопасности.

Кроме того, ежедневно по всему миру специалистами в области информационных технологий производится обнаружение новых уязвимостей в программном обеспечении, а также появляются новые виды вредоносного программного обеспечения, что дает основание для разработки и внедрения модуля обновления базы данных известных событий и инцидентов информационной безопасности.

Кроме того, для формирования отчетной документации по состоянию конкретного инцидента, или состоянию системы за некоторый отчетный период, необходимо внедрение модуля формирования отчетной документации.

Внедрение этих модулей в действующую систему хранения данных о событиях и инцидентах информационной безопасности позволит не только расширить возможности использования средств и активов центров информационной безопасности, но и сократить временной промежуток между этапом обнаружения и этапом реагирования на компьютерные инциденты.

Ключевые слова: информационная безопасность; система управления инцидентами; база данных; инцидент информационной безопасности; событие информационной безопасности.

ОСОБЕННОСТИ СИСТЕМНОГО И СЕТЕВОГО АДМИНИСТРИРОВАНИЯ ОПЕРАЦИОННОЙ СИСТЕМЫ ASTRA LINUX

Бунякина Екатерина Витальевна

*Военно-морской политехнический институт, Военный учебно-научный центр
Военно-Морского Флота «Военно-морская академия имени
Адмирала Флота Советского Союза Н.Г. Кузнецова»,
г. Санкт-Петербург, Россия school5572007@yandex.ru*

Комолова Нина Владимировна

*кандидат технических наук, доцент,
Военно-морской политехнический институт, Военный учебно-научный центр
Военно-Морского Флота «Военно-морская академия имени
Адмирала Флота Советского Союза Н.Г. Кузнецова»,
г. Санкт-Петербург, Россия, ninapetergof@mail.ru*

Яковлева Елена Сергеевна

*кандидат технических наук,
Военно-морской политехнический институт, Военный учебно-научный центр
Военно-Морского Флота «Военно-морская академия имени
Адмирала Флота Советского Союза Н.Г. Кузнецова»,
г. Санкт-Петербург, Россия, 2305elena@mail.ru*

Военно-профессиональная деятельность как в мирное, так и в военное время, является настолько сложной, многообразной и непредсказуемой, что, хотя управление военными объектами является прерогативой командиров, именно автоматизированные системы специального назначения вырабатывают рекомендации на управление военными объектами, помогающие командирам в принятии решений.

Автоматизированные системы специального назначения базируются на разных операционных системах, среди которых можно выделить два направления: операционные системы семейства Windows и операционные системы семейства Linux.

В последние годы правительством Российской Федерации выработан ряд документов, стимулирующих переход на отечественное программное обеспечение. В Военно-морском политехническом институте в рамках дисциплины «Операционные системы (ОС)» несколько лет назад перешли на обучение ОС МСВС и Astra Linux. Были опробованы релизы Astra Linux Орел и Astra Linux Смоленск. Так что будущие военные командиры приобрели навыки работы в современных отечественных операционных системах, умения администрирования операционных систем, и знания прав доступа к файлам и каталогам.

Системный администратор должен уметь, как установить операционную систему на отдельном компьютере, так и поддерживать устойчивую работу сетевой среды при больших нагрузках, сбоях в работе дисков и умышленных атак.

К задачам системного администратора относятся:

- инициализация пользователей;
- подключение и удаление аппаратных средств;
- резервное копирование;
- инсталляция и обновление программ;
- мониторинг системы;
- поиск неисправностей;
- слежение за безопасностью системы;
- оказание помощи пользователям.

Системный администратор отвечает за реализацию стратегии защиты и периодически проверяет, не нарушена ли безопасность системы. В системах с низким уровнем безопасности эта процедура может быть сведена к нескольким элементарным проверкам на предмет несанкционированного доступа. В системах с высоким уровнем безопасности обычно применяется сложная сеть ловушек и программ контроля.

Хотя профессиональные администраторы не являются разработчиками ОС, им приходится тратить много сил, аналитических способностей и знаний в области архитектуры компьютерных сетей для написания сценариев (scripts). Профессионалы могут читать и модифицировать сценарии, написанные на языке sh или bash интерпретаторов. Системный администратор должен устанавливать и настраивать серверную и клиентскую часть службы ssh в различных конфигурациях в соответствии с требованиями безопасности, а также организовать безопасный вход в систему, используя ключи.

Системный администратор проверяет состояние сервера ssh, исследуя конфигурационный файл: # /etc/init.d/ssh status. Предварительно проверяется, запущен или нет демон sshd: # ps ax|grep sshd.

Если он не запущен, запустить его следует посредством команды администратора:

```
# service sshd start
```

При подключении по ssh используются три вида аутентификации: аутентификации по паролю, по ключу хоста и по открытому ключу. Аутентификация по паролю в чистом виде является наиболее безопасной. При первом подключении с использованием аутентификации по ключу хоста открытый ключ хоста (сервера) копируется на компьютер-клиент в профиль пользователя, инициирующего удаленное подключение, в файл ./ssh/known_hosts. Настройки sshd находятся в файле /etc/ssh/ssh_config. Конфигурационный файл содержит следующие опции:

Port - по умолчанию используется 22 порт. Можно отредактировать значение порта. Изменим его, например, на нестандартный порт 2233 – это избавит сервер от сетевых роботов, которые автоматически сканируют интернет в поиске открытых портов и пытаются через них подключиться: Port 2203.

По умолчанию сервер «слушает» (принимает подключения) на всех сетевых интерфейсах. Можно оставить это значение по умолчанию:

```
#ListenAddress::
```

В этом файле есть группа параметров, относящихся к аутентификации. Параметр LoginGraceTime указывает количество секунд, через которое соединение будет разорвано, если пользователь не войдет в систему.

Все изменения сохраняются и служба sshd перезапускается. При подключении производится проверка, если всё в порядке, то настройка сервера ssh закончена.

Корректировка конфигурационных файлов системным администратором обеспечивает безопасную работу в операционной системе Astra Linux.

Ключевые слова: операционные системы; системный администратор; написание сценариев; служба ssh; безопасная работа в операционной системе Astra Linux.

ПОДХОД К ТЕСТИРОВАНИЮ НА ПРОНИКНОВЕНИЕ В ИНФОРМАЦИОННЫЕ СЕРВИСЫ СЕТИ RSNET ПО СКРЫТЫМ КАНАЛАМ, ОСНОВАННЫМ НА МЕТОДАХ СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ

Яндашевская Элина Андреевна

Академия Федеральной Службы Охраны России
г. Орел, Россия, elenayanda@yandex.ru

В настоящее время наблюдается все возрастающий рост компьютерных атак на объекты критической информационной инфраструктуры — совокупность автоматизированных систем управления технологическими процессами критически важных объектов Российской Федерации. Это связано, с одной стороны, с различным уровнем защищенности, а с другой — с доступностью информации об инструментах и методиках реализации компьютерных атак.

Одним из объектов критической информационной инфраструктуры является Единая сеть передачи данных для госорганов RSNet — сегмент сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Подключиться к RSNet может любой орган местного управления вплоть до городской администрации. Наличие подобной динамической инфраструктуры порождает проблему вероятных компьютерных атак на ее узлы, решение которой обеспечивает подсистема безопасности RSNet.

В рамках этой подсистемы разрабатывается Задание по безопасности, которое включает в себя: архитектуру и принципы взаимодействия подсистем информационных систем общего пользования; описание возможных нарушений целостности, устойчивости функционирования и безопасности; описание подсистемы безопасности, включая систему защиты информации и систему антивирусной защиты программных средств; непротиворечивую политику безопасности.

В зависимости от структуры и функций конкретного узла RSNet обеспечивается функции приема, хранения и обработки информации, представленной файлами различных документальных и мультимедийных форматов. Такие функции потенциально обеспечивают возможность реализации компьютерных атак различного типа, которые связанны в первую очередь с распространением вредоносного кода. Одним из таких методов распространения является использование скрытых информационных каналов, основанных на методах стеганографического преобразования информации. Причинами активного использования этих методов являются: возможность сокрытия не только самих данных, но и факта их загрузки/выгрузки; возможность обхода систем обнаружения вторжений; возможность обхода проверки в системах противодействия угрозам.

Указанные причины определяют актуальность проведения исследований компьютерных атак на основе методов стеганографического преобразования информации.

Целью представленного исследования является повышение защищенности информационных ресурсов узлов RSNet за счет реализации процесса тестирования

на проникновение по скрытым информационным каналам, основанным на методах стеганографического преобразования информации.

Предлагаемый тестовый стенд предназначен для планирования и проведения экспериментов, связанных с оцениванием потенциального ущерба вариантов узлов RSNet в ходе реализации атак по скрытым информационным каналам, основанным на методах стеганографического преобразования информации.

Наиболее целесообразным способом формирования вариантов программно-аппаратных реализаций узлов RSNet или их отдельных компонентов является использование технологии виртуализации, позволяющей достаточно оперативно создавать, хранить и развертывать образы компьютерных систем, которые составляют основу компонентов конкретного узла RSNet. Таким образом, хранилище виртуальных образов вариантов узлов RSNet или их отдельных компонентов может быть представлено совокупностью развернутых и сконфигурированных виртуальных машин.

Для имитации телекоммуникационной подсистемы, обеспечивающей их сетевое взаимодействие, а также взаимодействие с внешними сетями, целесообразно использовать технологию программно-конфигурируемой коммутации и маршрутизации.

Для поддержки функционирования указанных видов хранилищ, а также телекоммуникационной подсистемы в рамках предлагаемого тестового стенда должны быть развернуты соответствующие службы администрирования, поддерживаемые одним или более специалистами по поддержке распределенных информационных систем.

Кроме того, для реализации функции мониторинга уязвимости варианта скрытого информационного канала требуется развертывание подсистемы мониторинга, которая поддерживается специалистами по информационной безопасности. Соответственно, актуальным является рассмотрение методов формирования, методологических подходов к моделированию стеганографических систем, а также критериев принятия решения о наличии или отсутствии скрытого информационного канала. Для этого требуется проведение исследований методов и алгоритмов формирования скрытых каналов передачи информации, направленных на решение следующих классов частных задач: снижение вероятности обнаружения скрытого канала на основе стеганографического преобразования информации или факта передачи в нем скрытых сообщений; повышение пропускной способности; ресурсное и/или стоимостное оценивание эффективности данного скрытого канала; устойчивость канала к различным видам воздействия, как естественной природы, так и активного противодействия противника.

Актуальной задачей является рассмотрение возможности применения теоретико-информационного подхода к моделированию стеганографической системы с пассивным противником, с учетом необходимости решения обратной задачи, связанной со скрытностью передаваемых в ее рамках сообщений.

Ключевые слова: единая сеть передачи данных; скрытый канал; стеганографическое преобразование информации; теоретико-информационный подход; пассивный противник.

ПРИМЕНЕНИЕ ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСИ ДЛЯ ЗАЩИТЫ КОНТРОЛЬНОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Павлов Илья Павлович

Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко, г. Краснодар, Россия, pavlovvvv1989@gmail.com

В информационных системах не уделяется достаточного внимания на мониторинг и защиту контрольной информации и журналов событий информационной безопасности. Уровень защищенности хранимой контрольной информации должен быть достаточным для предотвращения любых изменений в любых данных, входящих в состав контрольной информации. Контрольная информация должна храниться защищенным образом согласно соответствующей политике информационной безопасности.

Для обеспечения целостности контрольной информации в информационной системе может использоваться простая электронная подпись, которая, при определенных условиях, приравнивается к собственноручной подписи и обладает юридической силой. Для этого необходимо, чтобы ключ простой электронной подписи применялся в соответствии с правилами, установленными оператором информационной системы, и в электронном документе содержалась информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ.

Для признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, необходимо соблюдение правил определения лица, подписывающего электронный документ, по его простой электронной подписи, а также выполнение обязанности лица, создающего и (или) использующего ключ простой электронной подписи, соблюдать его конфиденциальность.

Предлагаемая простая электронная подпись формируется следующим способом.

Сначала вырабатывается хэш-код от конкатенации логина и пароля пользователя, который используется как инициализационный вектор IV_1. Далее вычисляется IV_2 (второй инициализационный вектор). Для этого вырабатывается хэш-код от IV_1 и конкатенации идентификационного номера сотрудника в информационной системе организации IDP_i и метки времени t. После вычисления инициализационного вектора, мы можем сформировать простую электронную подпись $Sign_{ij}$ из подписываемого электронного документа M_j.

Предлагаемая простая электронная подпись является аналогом собственноручной подписи, в ней соблюдены правила определения лица, подписывающего электронный документ, по его простой электронной подписи, а также выполнено требование соблюдения конфиденциальности простой электронной подписи, кроме этого она не несёт в себе лишней информации (не нужны специальные криптографические средства для создания электронной подписи, нет нужды в удостоверяющем центре и сертификатах) и не требуется больших вычислений.

Ключевые слова: информационная система; информационные активы; контрольная информация; событие информационной безопасности; хэш-код; электронная подпись.

ПРОГНОЗИРОВАНИЕ ВРЕДОНОСНЫХ ВОЗДЕЙСТВИЙ (КОМПЬЮТЕРНЫХ АТАК) НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

Королев Игорь Дмитриевич

доктор технических наук, профессор,
Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
г. Краснодар, Россия, pi_korolev@mail.ru

Стадник Александр Николаевич

кандидат военных наук,
Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
г. Краснодар, Россия, alstaff@ya.ru

Алпеев Евгений Васильевич

Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
г. Краснодар, Россия, evolution-sipg@ya.ru

В настоящее время технологии, применяемые для распознавания аномальной активности, на практике демонстрируют недостаточность применения сочетания эвристических правил и наборов сигнатур для эффективной работы. Компьютерная атака представляет собой целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств. Типовая структура компьютерной атаки имеет комплексную и достаточно сложную организацию, полностью выявить и распознать которую сигнатурным способом без дополнительных инструментов детектирования будущих деструктивных воздействий достаточно сложно. С другой стороны, если говорить об анализе сетевого трафика и протекающих сетевых процессах, каждый анализируемый сетевой пакет это атомарное событие, предоставляющее определенную порцию информации, которую аналитическая система обнаружения компьютерных атак может использовать для решения следующих задач: оценки полноты контроля над текущей ситуацией в сетевой среде; предотвращения деструктивных воздействий по результатам обнаруженных следов или попыток совершения таковых воздействий; прогнозирования компьютерных атак с целью их предотвращения. Задача прогнозирования вредоносных воздействий (компьютерных атак) является важной с точки зрения предотвращения будущих атак со стороны нарушителя, как внутреннего, так и внешнего. С этой целью актуально описать процесс прогнозирования возможных вредоносных воздействий (компьютерных атак) на основе применения интеллектуального анализа данных. Для описания данного процесса, во-первых необходимо представить систему комплексного обнаружения компьютерных атак, во-вторых на базе данной системы описать процесс прогнозирования возможных вредоносных воздействий (компьютерных атак). Для построения классической системы обнаружения вредоносных воздействий (компьютерных атак), применяющей сигнатурный метод обнаружения в сочетании с эвристическими правилами, добавим интеллектуальный метод, который позволит прогнозировать ранее не выявленные воздействия на защищаемую систему. Совместное применение существующих баз безопасных и вредоносных объектов (сигнатур) и прогнозирования возможных вредоносных воздействий (компьютерных атак) в совокупности образуют систему комплексного обнаружения, которая в общем виде может состоять из следу-

ющих элементов: средства обнаружения подозрительных объектов, средства соблюдения политик безопасности, базы описаний подозрительных объектов, средства анализа объектов, базы данных безопасных объектов, базы данных вредоносных объектов (сценариев компьютерных атак), средства прогнозирования возможных вредоносных воздействий (компьютерных атак), базы данных прогнозируемых вредоносных воздействий (компьютерных атак). Процесс прогнозирования, с точки зрения применения в системе комплексного обнаружения вредоносных воздействий (компьютерных атак), включает следующие подпроцессы: формирование базы данных описаний подозрительных объектов, базы данных безопасных объектов, базы данных вредоносных объектов; интеллектуальный анализ баз данных безопасных объектов и вредоносных объектов и формирование базы данных прогнозируемых вредоносных воздействий; предоставление защищаемой системе набора эвристических правил для обнаружения подозрительных объектов, а также набора правил сбора информации посредством добавления соответствующей информации в базу описаний подозрительных объектов; на основании набора эвристических правил сбора информации об анализируемом объекте, предварительно ограничив доступ к объекту до получения результатов анализа; в случае если анализируемый объект не был признан подозрительным, в соответствии с вышеописанными эвристическими правилами, предоставляется доступ к блокируемому объекту; в случае, если объект был признан подозрительным, передается собранная информация для проведения его более глубокого анализа; далее происходит процесс получения запроса на передачу потенциально вредоносного объекта; в случае, если не получено разрешение на передачу упомянутого объекта, то анализ объекта прекращается и к нему предоставляется доступ; в случае если получено разрешение на передачу анализируемого объекта, производится передача указанного объекта для его глубокого анализа; далее, производится анализ переданного объекта с базой данных вредоносных объектов: если объект содержится в базе данных, то отправляется уведомление о том, что анализируемый объект является вредоносным, и формируются обновления эвристических правил для обнаружения подозрительных объектов и правила для устранения последствий присутствия вредоносных объектов в соответствии с результатами анализа, если нет, то переходит на следующий этап анализа переданного объекта с базой данных прогнозируемых вредоносных воздействий (компьютерных атак): если объект содержится в базе данных, то средство анализа объекта посылает уведомление о том, что анализируемый объект является вредоносным, и формирует обновления эвристических правил для обнаружения подозрительных объектов и правила для устранения последствий присутствия вредоносных объектов в соответствии с результатами анализа; если нет, то посылается соответствующее уведомление, в результате которого предоставляет доступ к объекту. Описанный процесс прогнозирования возможных вредоносных воздействий (компьютерных атак) на базе системы комплексного обнаружения защищаемой системы, демонстрирует поэтапную работу с подозрительным объектом (сценарием), начиная с момента отношения его к подозрительному, в соответствии с эвристическими правилами, последовательного сравнения подозрительного объекта (сценария) с каждой из описанных баз данных и отношения его либо к безопасному, либо к опасному, что является необходимым результатом.

Ключевые слова: компьютерная атак; интеллектуальный анализ; сигнатуры; эвристические правила; защищаемая система; подозрительный объект.

ПРОТОКОЛ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ТЕОРЕТИКО-ИНФОРМАЦИОННОЙ СТОЙКОСТЬЮ, ВЫПОЛНЯЕМЫЙ ПО ОТКРЫТЫМ И БЕСШУМНЫМ КАНАЛАМ СВЯЗИ

Коржик Валерий Иванович

*доктор технических наук, профессор,
Санкт-Петербургский государственный университет
телекоммуникаций имени проф. М. А. Бонч-Бруевича,
г. Санкт-Петербург, Россия, val_korzhik@yandex.ru*

Кабардов Муаед Мусович

*кандидат физико-математических наук, доцент,
Санкт-Петербургский государственный университет
телекоммуникаций имени проф. М. А. Бонч-Бруевича,
г. Санкт-Петербург, Россия*

Романова Ульяна Михайловна

*Санкт-Петербургский государственный университет
телекоммуникаций имени проф. М. А. Бонч-Бруевича,
г. Санкт-Петербург, Россия*

Леутин Евгений Игоревич

*Санкт-Петербургского государственного университета
телекоммуникаций имени проф. М.А.Бонч-Бруевича,
г. Санкт-Петербург, Россия*

Важным средством обеспечения информационной безопасности цифровых данных является использование стойких методов их шифрования при хранении и передаче по открытым каналам связи. В настоящее время известен ряд стандартов шифрования, которые являются вычислительно стойкими, однако, только лишь этим не закрывается проблема информационной безопасности, поскольку корреспонденты, пользующиеся подобными шифрами, должны быть обеспечены для них ключевыми данными.

Известно множество протоколов обмена информацией между пользователями, которые, казалось бы, позволяют решить эту проблему. Однако, оказывается, что все они не лишены определенных недостатков. Так часть протоколов требуют от пользователей наличия связи с доверенными удостоверяющими центрами, что приводит пользователей к зависимости от доверительности таких центров, а также требует значительных затрат времени и средств.

В данной работе рассматривается протокол, который из известных нам протоколов, впервые обеспечивает заранее заданные условия на достоверность передачи данных по основному каналу и утечку по каналу перехвата. В отличие от ранее известных протоколов подобного типа он не предполагает никаких условий, накладываемых на канал перехвата. Секретность данного протокола не требует никаких криптографических предположений, в частности невозможности факторизации больших чисел или выполнения дискретного логарифмирования, и поэтому он сохраняет свою стойкость даже при условии практической реализации квантовых компьютеров. В качестве основного канала и канала перехвата рассматривается открытый бесшумный канал с постоянными параметрами, типичным примером которых является обычный Интернет. Интерес к рассмотрению именно такого канала состоит в том, что он доступен для обычных пользователей, имеющих в своем распоряжении

лишь персональные компьютеры (ПК). Это позволит им обеспечить обмен конфиденциальной информации, получив алгоритм шифрования/дешифрования как известные стандарты из того же Интернета.

Однако, выполнение данного протокола требует достаточно интенсивного обмена данными по каналам связи. Поэтому основной акцент в данной работе делается на расчет требуемого трафика такого обмена, в зависимости от размеров распределяемых ключей и других параметров протоколов. Результаты эксперимента и расчета показали, что этот трафик все же вполне приемлем для пользователей, имеющих обычные персональные компьютеры. Единственным дополнением к необходимому программному обеспечению должно быть такое аппаратное устройство, как датчик случайных чисел. В работе экспериментально исследуются требуемые свойства такого датчика и делается вывод о его пригодности с использованием отечественных устройств.

Дальнейшие направления исследований могут быть связаны с дальнейшим упрощением процедуры протокола, сокращением трафика обмена, с увеличением объема ключевых данных, а также с обеспечением защиты от активного перехвата.

Ключевые слова: ключевые данные; открытый бесшумный канал; случайные числа; квантовые компьютеры.

РАЗРАБОТКА МЕТОДИКИ ВНЕДРЕНИЯ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ WEB-ПРИЛОЖЕНИЯ

Ковцур Максим Михайлович

кандидат технических наук, доцент,
Санкт-Петербургский государственный университет телекоммуникаций
имени проф. М.А.Бонч-Бруевича, г. Санкт-Петербург, Россия, maxkovzur@mail.ru

Кириллов Даниил Игоревич

Санкт-Петербургский государственный университет телекоммуникаций
имени проф. М.А.Бонч-Бруевича, г. Санкт-Петербург, Россия, daniil.kirillov@gmail.com

Михайлова Анастасия Валерьевна

Санкт-Петербургский государственный университет телекоммуникаций
имени проф. М.А.Бонч-Бруевича, г. Санкт-Петербург, Россия, ova.007@yandex.ru

Потемкин Павел Андреевич

Санкт-Петербургский государственный университет
телекоммуникаций имени профессора М.А.Бонч-Бруевича.
г. Санкт-Петербург, Россия, potiomkinpa98@gmail.com

Каждый человек по статистике проводит порядка 6 часов в сети Интернет, переходя по различным web-страницам, общаясь в социальных сетях, скачивая файлы. В 21 веке пользователи используют миллиарды web-приложений, обеспечивающих выполнения множества функций. По причине их популярности и удоб-

ства они ежедневно подвергаются различным атакам со стороны нарушителей. Большинство web-приложений имеют низкий уровень защищенности. Поэтому использование Машинного обучения, в перспективе, может решить сразу две задачи - автоматизация процессов, которые ранее требовали участия человека и быстрая обработка, с последующим анализом огромных объемов информации и расчёт параметров, используя множество переменных. Для обеспечения информационной безопасности существуют различные механизмы и технологии. Классическое представление безопасного web-приложения представляет собой систему, включающую следующие аспекты — разграничение прав доступа, использования механизмов защиты баз данных от извлечения информации, постоянный поиск уязвимостей web-приложений, использование новых технологий обеспечения непрерывной работы сервера. С каждым днём Машинное обучение внедряют в больших масштабах в различные отросли информационных технологий - телекоммуникации, финансы, транспорт, производство и даже сельское хозяйство. На данный момент, обеспечение компьютерной безопасности является приоритетной задачей для всего мира. Использование машинного обучения позволит вводить новые потенциальные решения, независимо от сложности их реализации или затрате ресурсов, данный метод позволит автоматизировать любой процесс в любой области деятельности. Применение этой технологии в компьютерной и информационной безопасности, позволит обеспечить защиту и эффективную работу интернет ресурсов на основе которых, и совершенствуется технология Машинного обучения.

Одной из главных метрик эффективной работы умных сетей является критерий качества разработанной модели. При определении наиболее значимых параметров метода обучения, признаков и свойств модели необходимо формализовать критерий определения качества, на основе которого будет производится усовершенствование и оптимизация рассматриваемого процесса. Для этого можно использовать средний модуль ошибки оценки полученного прогноза, также может быть использована вероятность ошибки классификации. Для построения наиболее эффективной модели необходимо обеспечить наиболее точный выбранный критерий, на основе которого можно будет определить реальные потери или выигрыш на практике. Но анализировать среднее отклонение результатов прогнозирования и фактическими значениями необходимо на внешних данных, которые не были настроены для калибровки построенной модели, при этом не используя для сравнения обучающей выборки, в противном случае возможно появления проблемы переобучения. На каждом этапе обучения необходимо оценивать среднее качество результатов прогнозирования на предмет точности, чтобы обеспечить качественные итоговые результаты обучения. Использование кросс-валидации позволит обеспечить лучшие результаты, а именно оценку разброса в точности предсказания модели, также обеспечить проверку модели на предмет того, насколько статистически значимым является отличие точности одной модели от другой. При введении кросс-валидации в модель предсказания вся обучающая выборка делится на число случайных частей, из-за чего происходит искажения отдельных частей тренировочной выборки и отсутствие прежней структуры исходных данных. Для решения данной проблемы необходимо чтобы, все части обучающей выборки как можно более реалистично отражали всю полноту информации, поэтому случайное разбиение, как правило, необходимо производить стратифицировано, то есть сохраняя пропорции классов, а также сохраняя пропорций значений отдельных признаков во всех частях разбиения выборки. При оценке модели важно выбирать качественные признаки, доступные для измерения в момент прогнозирования, это позволит по-

лучить наиболее эффективную модель машинного обучения. Целью данной работы является разработка модели машинного обучения, обеспечивающая информационную безопасность web-приложения.

Ключевые слова: web-приложение; сервер; машинное обучение; аномально поведение; учетная запись; пользователь.

СИСТЕМА ФУНКЦИОНАЛЬНЫХ И МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Конышев Евгений Александрович

*Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
г. Краснодар, Россия, vire-more@mail.ru*

Необходимость обеспечения защиты информации в автоматизированных системах специального назначения от деструктивного воздействия вредоносного программного обеспечения привела к внедрению в практику широкой номенклатуры антивирусных механизмов, которые можно разделить на два класса: антивирусные механизмы резидентного и сеансового типа. Достоинством механизмов антивирусной защиты сеансового типа является их простота, связанная с независимостью реализуемых функций от функций программного обеспечения автоматизированных систем специального назначения и, как следствие - возможность управления временными ресурсами автоматизированных систем специального назначения за счет инициирования работы антивирусных механизмов администратором, Недостатком данной технологии является следующее – защищенность информации обеспечивается лишь периодически, во время реализации сеансов применения данных антивирусных механизмов. Преимуществом механизмов антивирусной защиты резидентного типа является своевременное реагирование на некорректное состояние технологической среды средств вычислительной техники автоматизированных систем специального назначения, вследствие воздействия вредоносного программного обеспечения,. Вместе с тем, применение механизмов антивирусной защиты резидентного типа влечет необходимость одновременного использования с программным обеспечением автоматизированных систем специального назначения ее временного ресурса, что является предпосылкой конфликта по использованию данного ресурса указанными механизмами с различными целевыми функциями автоматизированных систем специального назначения. Исходя из вышеизложенного, возникает необходимость решения ряда задач по оптимизации, связанных с определением минимально возможной величины объема временного ресурса, необходимого для использования механизмами антивирусной защиты резидентного типа, и проведения комплексного моделирова-

ния информационных процессов в автоматизированных системах специального назначения в условиях применения антивирусных механизмов резидентного типа и деструктивного воздействия вредоносного программного обеспечения. Указанное комплексное моделирование, сопряжено с необходимостью их функционального описания. Такое описание возможно получить в рамках методологии функционального моделирования. Функциональная модель представляет собой иерархическую систему выполняемых предметных функций, отражающих свои взаимоотношения через информацию о системе. В основу функционального моделирования положена декомпозиция предметной целевой функции и ее последовательная детализация, начиная с общего описания. Функциональная модель нулевого уровня представляет собой целевую (системную) функцию «Информационные процессы в автоматизированных системах специального назначения в условиях применения антивирусных механизмов резидентного типа и деструктивного воздействия ВПО». Дальнейшая декомпозиция целевой (системной) функции и ее иерархическая детализация позволяет выявить полный набор подфункций, в данном случае функциональная модель первого уровня содержит три частные функции: «Функционирование автоматизированных систем специального назначения по целевому назначению», «Деструктивное воздействие вредоносного программного обеспечения на информационные процессы в автоматизированных системах специального назначения» и «Защита информации антивирусными механизмами резидентного типа от воздействия угроз безопасности информации, реализуемых вредоносным программным обеспечением». Функциональная модель второго уровня содержит 10 локальных целевых функций. Третий уровень декомпозиции целевой (системной) функции будет являться конечным, и представляется 37 локальными целевыми функциями. Полученное функциональное описание позволяет сформировать соответствующие аналитические выражения для определения средних значений композиций случайных величин исследуемых характеристик. Построение указанных аналитических выражений основывается на аддитивности математического ожидания композиции случайных величин обладающих свойством линейности. Полученные аналитические выражения будут являться математическими моделями средних значений случайных величин времени реализации информационных процессов в автоматизированных системах специального назначения в условиях применения антивирусных механизмов резидентного типа и деструктивного воздействия вредоносного программного обеспечения. Целью данной работы является построение системы функциональных и математических моделей информационных процессов в автоматизированных системах специального назначения в условиях применения антивирусных механизмов резидентного типа и деструктивного воздействия вредоносного программного обеспечения.

Ключевые слова: антивирусные механизмы; функциональное моделирование; математическое моделирование.

СОВМЕЩЕНИЕ АЛГОРИТМОВ ФУНКЦИОНИРОВАНИЯ РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАДЕЙСТВОВАННЫХ РЕСУРСОВ

Гнутов Максим Сергеевич

*Краснодарское высшее военное о училище имени генерала армии С.М. Штеменко,
г. Краснодар, Россия, monk666@bk.ru*

Тенденции развития информационных технологий приводят к росту топологии сетей различных уровней. Как следствие, изолированные автоматизированные системы, как таковые, уходят в прошлое. Увеличение информационного обмена, задействование ряда специалистов и различных подсистем, необходимых в достижении цели, преобразуют автоматизированные системы в распределенные автоматизированные системы. В распределенных автоматизированных системах происходит увеличение потребления ресурсов — дополнительные затраты на обеспечение обмена информацией в сети, обеспечение безопасности информации, контроль доступа и т.д. Для обеспечения безопасного и своевременного выполнения задач в распределенных автоматизированных системах необходимо либо увеличение производительности комплекса средств автоматизации, либо реконфигурация алгоритмов функционирования данных систем за счет использования незадействованных ресурсов.

Математические вычисления на графических процессорах могут применяться в достаточно небольшом спектре задач из за упрощенной архитектуры ядер. Однако, простые массовые параллельные вычисления под силу графическим вычислителям.

Любой набор процессов, стартующих в информационной системе, последовательно использует конечное количество системных ресурсов. Для каждого элемента множества системных ресурсов имеется некий фактор, определяющий очередность исполнения того или иного процесса, т.е. его приоритет. Зададим алгоритм выбора запуска приоритетного процесса с помощью графа. Любой граф алгоритма можно преобразовать в ярусно-параллельную форму. Максимального ускорения можно добиться, увеличивая ширину ярусно-параллельной формы представления алгоритма и уменьшая ее высоту (количество ярусов является ничем иным, как количеством тактов). С помощью разноцветных сетей Петри представим выполнение набора процессов Pr_n, как смену состояний элементов (процессов) через переходы t_n под влиянием множества факторов f_n.

Для увеличения доли последовательных операций и получения максимального ускорения по закону Амдала, после вычисления высоты канонической ярусно-параллельной формы (поиска кратчайшего пути), будем использовать эквивалентное преобразование (например, суммирование элементов массива, выполненное последовательно за 7 тактов, параллельно вычисляется всего за 4). Совместное использование методов представления и преобразования алгоритмов в условиях избытка незадействованных вычислительных ресурсов графического процессора дает значительное ускорение работы распределенных автоматизированных систем за счет параллельных вычислений и достаточно компактной формы алгоритма.

Ключевые слова: разноцветные сети Петри; ярусно-параллельная форма представления алгоритма; эквивалентное преобразование; граф алгоритма; закон Амдала.

СПОСОБ ПОВЫШЕНИЯ СТОЙКОСТИ МНОГОФАКТОРНОЙ БИОМЕТРИЧЕСКОЙ ПОРОГОВОЙ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ

Казарин Михаил Андреевич

*Военная академия связи имени Маршала Советского Союза С. М. Буденного,
г. Санкт-Петербург, Россия, kazarinmisha@mail.ru*

Липатников Валерий Алексеевич

*доктор технических наук, профессор, СНС,
Военная академия связи имени Маршала Советского Союза С. М. Буденного,
г. Санкт-Петербург, Россия, lipatnikovanl@mail.ru*

Сахаров Дмитрий Владимирович

*кандидат технических наук, доцент,
Санкт-Петербургский государственный университет телекоммуникаций
имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, sguard7@mail.ru*

Традиционные способы аутентификации пользователей информационных систем (ИС) защищены недостаточно. Применяемые при этом специальные меры неэффективны для защиты ИС от несанкционированного доступа (НСД) из-за слабой стойкости средств авторизации. Более эффективную авторизацию обеспечивает биометрия, использующая оригинальные атрибуты тела человека. На стыке биометрии и криптографии сформировалось научное направление «биокриптография». Биометрическая аутентификация персональных данных широко используется для разблокировки устройств, входа в приложение, доступа в информационную систему, мобильного платежа, доступа в закрытое помещение и т.д. Данный вид аутентификации предоставляет удобный способ подтвердить свою подлинность, так как по сравнению с традиционными методами не требует запоминания пароля и не зависит физических устройств. Вследствие использования биометрии в системах обработки защищаемой информации (автоматизированные системы управления специального назначения, объекты критической инфраструктуры, банковская сфера и др.) атаки на биометрические системы аутентификации совершенствуются и они могут быть скомпрометированы.

У технологии биометрической аутентификации есть особенности, которые несут дополнительные угрозы конфиденциальности: публичность биометрических данных, которые можно легко найти в сети, например, фотографии, видеозаписи и голос человека и использовать их для аутентификации; при компрометации биометрического эталона безопасность всей системы ставится под угрозу, так как в отличие от пароля или смарт-карты невозможно заменить лицо, голос, радужную оболочку; невозможно применять биометрическую аутентификацию для людей с физическими недостатками.

Обмануть систему можно на этапе регистрации, внеся в систему чужие биометрические данные, в момент верификации украсть базу биометрических образцов (слепков или предъявить фото, запись голоса или силиконовый слепок отпечатка пальца) или вмешаться в процесс принятия решения о допуске пользователя в систему.

Биометрические эталоны хранятся в базах данных (БД) в зашифрованном виде, оператор контролирует их ввод и проверяет идентичность. Наиболее опасной является атака типа спуфинг, при которой злоумышленник на этапе верификации выдает себя за легитимного пользователя.

Каждый компонент биометрической системы потенциально уязвим. Для это используют: размещение поддельной биометрии на датчике, полученной неавторизованным способом (создание поддельного липкого пальца, распечатка радужной оболочки, маска для лица); повторную передачу ранее сохраненных оцифрованных биометрических сигналов. Ранее сохраненный в БД сигнал воспроизводится в системе в обход устройств сбора данных; переопределение процесса извлечения объектов. Предварительно выбранный шаблон создается в модуле извлечения объектов с использованием троянского коня.

Объектом исследования является система биометрической криптографической аутентификации пользователей информационной системы, предметом — процесс аутентификации на основе пороговой схемы. Цель исследования — снижение вероятности ошибки 2 рода (пропуск цели). Результат: Разработан способ повышения стойкости многофакторной биометрической пороговой криптографической системы аутентификации пользователей на основе нейросетевых алгоритмов и метода выявления живучести («liveness detection»).

В предложенном способе в целях повышения стойкости к различным атакам и защиты от фальсификации пользователь выполняет дополнительные инструкции для доказательства своей аутотентичности. Применяются комбинации различных методов аутентификации (статических и динамических) и, в отличие от известных, к динамическим методам защиты добавлены процессы на основе нейросетевых алгоритмов и технологии «liveness detection», что позволяет снизить вероятность ошибки системы и повысить ее стойкость. Указанная технология подтверждает, что аутентификацию проходит живой человек, а не его маска.

Способ работает следующим образом. Пользователь вводит свои биометрические данные посредством соответствующего сканера (прикладывает палец, говорит в микрофон, расписывается, смотрит в камеру). Далее система требует выполнения определенных инструкций от пользователя для подтверждения его подлинности, например, повторить случайные фразы или последовательность чисел с экрана, написать что-то, моргнуть, улыбнуться, повернуть голову. Затем идет преобразование введенных данных в цифровой код методом «нейронных сетей».

Система анализирует введенные данные и действия пользователя, сравнивает их с эталонами в БД. Если введенные данные совпадают с шаблонами в БД, то доступ в систему разрешен, иначе — отказ.

Вывод. Предложенный способ в отличие от известных имеет большую стойкость многофакторной биометрической пороговой криптографической системы к различным атакам за счет применения нейросетевых алгоритмов и технологии «liveness detection» и позволяет повысить результативность аутентификации пользователей. Практическая значимость: предлагаемый способ применим для систем с высоким уровнем защиты в автоматизированных системах управления специального назначения.

Цель исследования по снижению вероятности пропуска цели (возникновения ошибки 2 рода) достигнута.

Ключевые слова: информационные системы (ИС); несанкционированный доступ (НСД); базы данных (БД); аутентификация; угрозы биометрической аутентификации; биометрические персональные данные; пороговые схемы; многофакторная биометрическая система; нейросетевые алгоритмы; метод выявления живости.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТЕГОСИСТЕМ С ВЛОЖЕНИЕМ В НАИМЕНЬШИЕ ЗНАЧАЩИЕ БИТЫ С СОГЛАСОВАНИЕМ И С ЗАМЕЩЕНИЕМ

Ахрамеева Ксения Андреевна

кандидат технических наук,
Санкт-Петербургский государственный университет телекоммуникации имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, oklaba@mail.ru

Герлинг Екатерина Юрьевна

кандидат технических наук,
Санкт-Петербургский государственный университет телекоммуникаций имени проф. М. А. Бонч-Бруевича, г. Санкт-Петербург, Россия, gerlingeu@gmail.com

В нынешний век стремительного развития технологий как никогда остро встает вопрос сохранения и защиты конфиденциальной информации от посягательств злоумышленников. Не смотря на то, что методы стеганографии использовались со времен Геродота, в настоящее время стеганографические методы модернизировались в цифровой вид и используются для хранения и передачи информации, скрытно от посторонних лиц. На сегодняшний день, существует множество методов по вложению и передачи дополнительной информации в цифровом виде. Чаще всего используются вложения в обычный, ничем не примечательный файл — покрывающий объект. После погружения информации в покрывающий объект — такой файл называется стеганограммой или стегообъектом. В качестве покрывающих объектов могут использоваться любые медиафайлы, такие как фото, видео, аудио, текст. Наиболее легким и часто используемым методом вложения в фото, видео и аудио файлы является метод вложения в наименьший значащий бит и его разновидности. Необходимо определить принципиальные различия процедуры вложения дополнительной информации в покрывающий объект для стегосистем с вложением в наименьшие значащие биты с замещением и с согласованием. Наиболее популярным контентом в сети Интернет являются неподвижные изображения, такие как фотографии и картинки. В связи с этим, представляет интерес рассмотреть стегосистемы с вложением в наименьшие значащие биты, в качестве покрывающих объектов для которых выбраны статические изображения. Различные алгоритмы процедуры вложения в наименьшие значащие биты с замещением и согласованием приводят к различным статистическим признакам стегообъектов, что сказывается на их стойкости к стегоанализу. Исследована стойкость рассматриваемых стегосистем относительно методов стегоанализа таких как визуальная атака, атака на основе статистики первого порядка (атака хи-квадрат), атака на основе статистики второго порядка (парно-выборочный анализ). Целью данной работы является нахождение принципиальных различий между рассматриваемыми стегосистемами для оптимизации их использования и повышения эффективности использования стегосистем с вложением в наименьшие значащие биты относительно информационной безопасности.

Ключевые слова: стеганография; вложение в наименьшие значащие биты; стегоанализ; покрывающий объект; стеганограмма.

ТЕОРЕТИЧЕСКАЯ ОЦЕНКА ИСПОЛЬЗОВАНИЯ МАТЕМАТИЧЕСКИХ МЕТОДОВ ПРОГНОЗИРОВАНИЯ ЗАГРУЗКИ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

Шемякин Сергей Николаевич

кандидат технических наук, доцент,
Санкт-Петербургский Государственный университет телекоммуникаций
имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, s4421764@yandex.ru

Пестов Игорь Евгеньевич

Санкт-Петербургский Государственный университет телекоммуникаций
имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, Pestovie@outlook.com

Ильин Максим Владимирович

Санкт-Петербургский Государственный университет телекоммуникаций
имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, forses3@mail.ru

Рудченко Никита Андреевич

Санкт-Петербургский Государственный университет телекоммуникаций
имени проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, rudebxy@yandex.ru

В наши дни виртуализация используется повсеместно, а особенно необходима для создания сетевой и серверной инфраструктуры предприятия. Без проведения математического прогнозирования невозможно точно предугадать поведение инфраструктуры через какой-то период времени. Следовательно, была поставлена задача – создать максимально точный прогноз на максимально длительный срок.

Для создания прогноза была выбрана модель авторегрессионного интегрированного скользящего среднего, основанная на временных рядах. У данной модели существует несколько различных доработок, таких как статная модель, расширенная модель, сезонная модель.

Рассмотрено описание математических моделей авторегрессионного интегрированного скользящего среднего, а так же расширенная модель авторегрессионного интегрированного скользящего среднего и сезонной модели авторегрессионного интегрированного скользящего среднего. На основании математического описания было произведено изучение методов прогнозирования и их сравнение. Затем методы математического прогнозирования были реализованы программно, построены графики, проведено сравнение и был выявлен лучший их них для прогнозирования поведения сетевой инфраструктуры.

Проведенные тесты показали, что модель авторегрессионного интегрированного скользящего среднего прогнозирует поведение сетевой инфраструктуры на неделю, расширенная модель авторегрессионного интегрированного скользящего среднего прогнозирует поведение сетевой инфраструктуры на месяц, а сезонная модель авторегрессионного интегрированного скользящего среднего прогнозирует поведение сетевой инфраструктуры на год.

Полученные результаты по итогам моделирования математического прогнозирования Бокса-Дженкинса имеют широкое практическое применение для мониторинга загрузки элементов виртуальной инфраструктуры, с целью предотвращения сбоев в работе системы и отслеживания аномалий, что повышает эффективность использования ресурсов и безопасность инфраструктуры.

Ключевые слова: arima; arimax; sarima; прогнозиование; временные ряды.

ФОРМАЛИЗАЦИЯ ИНФОРМАЦИОННОГО КОНФЛИКТА НА ОСНОВЕ ТЕОРИИ ДИНАМИЧЕСКИХ СИСТЕМ

Мамончикова Алина Сергеевна

публичное акционерное общество
«Информационные телекоммуникационные технологии»,
г. Санкт-Петербург, Россия, alinitta33@mail.ru

Телекоммуникационная система функционирует в условиях информационно-технических воздействий и технических средств разведки. Важным понятием в рассматриваемой области является «информационный конфликт», который формализует совместное воздействие технических средств разведки и информационно-технических воздействий на телекоммуникационную систему. Для моделирования информационного конфликта может быть использован научно-методический аппарат, основанный на различных теориях, а, именно: теория марковских процессов; теория сетей Петри; теория стохастических сетей; теория игр; теория сложных иерархических систем и др. Однако, формализация информационного конфликта с помощью перечисленных НМА не учитывает динамические характеристики процессов информационного конфликта. Известны работы ученых специалистов, в которых рассматривается актуальное направление исследований информационного конфликта, основанное именно на научно-методическом аппарате теории динамических систем. Отличительной особенностью этих работ является то, что в основу положены модели антогонистических двусторонних конфликтов, при этом модели трех и более сторон (многостороннего) информационного конфликта не рассматриваются. Таким образом, недостаточно изученными остаются динамические процессы информационного конфликта в условиях совместного влияния средств дестабилизирующих воздействий и технических средств разведки на телекоммуникационную систему. Целью работы является построение модели трехстороннего динамического информационного конфликта, на основе математического аппарата теории динамических систем. Впервые для разрабатываемой модели представлены три стороны динамического конфликта, учитывающие динамику развития информационного конфликта во времени, различные степени конфликтного взаимодействия отдельных сторон, представлен синтез универсальных подходов, обобщающих динамический информационный конфликт трех сторон. На сегодняшний день достигнуто решение двух частных научных задач: разработаны обобщенная и частная модели трехстороннего динамического информационного конфликта. К перспективным направлениям развития полученных моделей можно отнести следующее - исследование динамических конфликтов с более сложными вариантами конфликтного взаимодействия сторон и более глубоким изучением влияния сценариев поведения сторон на развитие и итог информационного конфликта.

Ключевые слова: динамический конфликт; динамические системы; формализация конфликта; информационный конфликт; многосторонний динамический конфликт.

ФОРМАЛИЗАЦИЯ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Маньков Евгений Александрович

*Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
г. Краснодар, Россия, emankov@inbox.ru*

Для формализации параметров оценки защищенности речевой информации на объектах информатизации специального назначения как оптимизируемых параметров и повышения защищенности речевой информации от утечки по техническим каналам. Рассмотрим характеристики информационной деятельности объектов информатизации специального назначения: защищенности речевой информации от утечки по техническим каналам, действий нарушителя по реализации угроз перехвата речевой информации (утечки по техническим каналам) и характеристики мер противодействия перехвату речевой информации нарушителем. Основанием для адекватной оценки этих характеристик служат следующие соответствия: соответствие информационных процессов условиям функционирования объектов информатизации специального назначения, соответствие условиям своевременной реализации процедур оценки защищенности речевой информации, соответствие периода оценки периоду возникновения угроз перехвата речевой информации (утечки техническим по каналам) и соответствие возможностей нарушителя безопасности информации по перехвату речевой информации. Данные характеристики будут служить параметрами для определения меры эффективности соответствующих им процедур в рамках выполнения целевой функции объектов информатизации специального назначения. Согласно теории информации такая интерпретация означает, что для определения характеристик информационной деятельности: – защищенности речевой информации от утечки по техническим каналам, действий по реализации угроз перехвата речевой информации (утечки по техническим каналам), а также характеристик мер противодействия перехвату речевой информации нарушителем, необходимо оценить свойства процедур накопления, обработки и обмена речевой информации, механизмов реализации угроз перехвата речевой информации (утечки по техническим каналам) и механизмов противодействия перехвату речевой информации нарушителем. Следует также отметить, что все вышеперечисленные механизмы являются унифицированными, так как реализуются в отношении общего объекта — речевой информации. Упрощенно алгоритм оценки заключается в присвоении заданным характеристикам определенных значений, при соблюдении единой метрики. Такой подход позволяет однозначно измерить характеристики информационной деятельности: – защищенности речевой информации от утечки по техническим каналам, действий по реализации угроз перехвата речевой информации (утечки по техническим каналам), а также характеристик мер противодействия перехвату речевой информации нарушителем. Однозначность измерения указанных характеристик определяется единицей измерения и достигается конечным числом: способов измерения, мер измерения и шкал измерения. Возникает необходимость обоснования требований к областям допустимых значений характеристик исследуемых процессов, для формирования множества таких характеристик, с точки зрения реализуемых функций и разработки соответствующих методик и моделей оценки. В зависимости от способа оценки характеристик

исследуемых процессов — измерение или вычисление, множество таких характеристик, будет представлено либо измеряемыми параметрами, либо вычисляемыми показателями. Измеряемый параметр обусловлен метрикой измерения и значениями измерений, таким образом, оценка измеряемого параметра является его объективной характеристикой. Измеряемому параметру присущи детерминированность области допустимых значений и измерительный инструментарий. Для информационных процессов объектов информатизации специального назначения, унифицированным измеряемым параметром будет время реализации процедур накопления, обработки, обмена речевой информации, перехвата речевой информации (утечки по техническим каналам) и процедур оценки противодействия перехвату речевой информации нарушителем, а унифицированным вычисляемым параметром — полнота реализации соответствующих процедур. Для процессов перехвата речевой информации (утечки по техническим каналам), унифицированным измеряемым параметром, является время реализации угроз перехвата речевой информации (утечки по техническим каналам), а для процессов противодействия перехвату речевой информации нарушителем — время реализации мероприятий противодействия. Унифицированным вычисляемым параметром для указанных процедур будет полнота их реализации. Для оценки эффективности информационных процессов объектов информатизации специального назначения примем показатель полноты реализации соответствующих функций. Таким образом показатель защищенности речевой информации на объектах информатизации специального назначения можно рассматривать как производный от полноты реализации целевых функций противника и целевых функций объекта информатизации, в частности полноты реализации угроз перехвата речевой информации противником (утечки по техническим каналам), и полноты реализации мер противодействия перехвату речевой информации нарушителем. Целью данной работы является формализация процессов обеспечения защиты речевой информации на объектах информатизации специального назначения, формирование задачи построения системы функциональных и математических моделей процессов перехвата речевой информации и процессов защиты речевой информации на объектах информатизации специального назначения.

Ключевые слова: речевая информация; объект информатизации специального назначения; информационные процессы.

СЕКЦИЯ № 4

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И СРЕДСТВ ПРИ РАЗРАБОТКЕ, ТЕХНИЧЕСКОМ ОБЕСПЕЧЕНИИ И ЭКСПЛУАТАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ И СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ РЛС В РАЗРАБАТЫВАЕМОЙ САПР РЛС И ПЕРСПЕКТИВЫ ЕГО ПЕРЕВОДА НА ТЕХНОЛОГИЮ HLA IEEE-1516

Коновальчик Артем Павлович

кандидат технических наук,
акционерное общество «Концерн Воздушно-Космической Обороны „Алмаз-Антей“»,
г. Москва, Россия, konovalchik@almaz-antey.ru

Щирый Андрей Олегович

кандидат технических наук,
акционерное общество «Концерн Воздушно-Космической Обороны „Алмаз-Антей“»,
г. Москва, Россия, andreyschiriy@almaz-antey.ru

В докладе показана общая архитектура разрабатываемой отечественной системы автоматизированного проектирования (САПР) радиолокационных станций (РЛС). Специфика разрабатываемой системы наиболее выражена в учете конкретных условий боевого применения, характеристик средств воздушно-космического нападения, фоноцелевой обстановки, для чего реализуется функционал имитационного моделирования боевых действий. Исходными данными для такого моделирования должны быть тактико-технические требования к разрабатываемым перспективным образцам вооружений и военной техники, а также принципы их боевого применения.

Основное внимание уделено построению детальной имитационной модели универсальной РЛС. Весь процесс проектирования РЛС концептуально структурирован в виде пяти уровней проектирования (системный, структурный, логический, схемотехнический, конструктивно-технологический уровни). При этом реализуется поддержка двух схем имитационного моделирования: на системном и структурном уровнях – по дискретно-событийной схеме, а на логическом уровне – по пошаговой схеме. Пошаговая схема обладает такими преимуществами, как простота и наглядность, в ней удобно моделировать алгоритмы обработки, составные части РЛС, и даже некоторые несложные виды РЛС. Однако, в ней невозможно корректное моделирование, например, РЛС с параллельной обработкой сигналов на разных частотах. Тем более в ней крайне ограничены возможности для моделирования группировок

войск и боевых действий. Поэтому при имитационном моделировании функционируют два планировщика: «высокоуровневый» дискретно-событийный диспетчер и «низкоуровневый» пошаговый. Дискретно-событийный диспетчер взаимодействует с пошаговым планировщиком каждый раз, когда рассчитывает очередной событийный блок одного из двух верхних уровней.

Для реализации дискретно-событийной схемы ведется динамическая очередь задач («календарь»), управляемая диспетчером имитационного моделирования, который определяет порядок передачи управления между вычислительными блоками (агентами, частными моделями — в других терминах). Это делается для синхронизации «модельного времени», причем в условиях, когда вычислительные блоки «шагают» по времени исходя из своей внутренней логики, временными интервалами произвольного размера.

Различия моделирований на системном и структурном уровнях заключаются в следующем. Системный уровень предназначен для анализа результатов моделирования, и ориентирован на оптимизацию размещения РЛС, объединение их в комплексы и системы с разветвлённой иерархией командных пунктов, отработку различных вариантов воздушного нападения, построение траекторий и оснащения объектов на радиосцене. На системном уровне задаются координаты стояния, тип РЛС (роль в группе), количество и координаты антенн, их тип, а также система управления из связанных командных пунктов и средств объединения РЛС в комплексы и системы. Решаются задачи анализа эффективности объединения РЛС в комплексы и системы, эффективности взаимодействия внутри группы. Настройка расположения РЛС, траекторий объектов наблюдения. Эффективность использования разнесённых антенн с учётом подстилающей поверхности, климатических особенностей сценария и пр.

Структурный уровень моделирования — это набор программных средств и средств анализа результатов моделирования, ориентированный на оптимизацию параметров приёмных и передающих трактов РЛС, модулей управления антеннами и антенными решетками, управления модуляцией зондирующего сигнала (ЗС). Предполагается, что облик оптимизируемой РЛС и требования к её техническим параметрам определены на системном уровне, а структурный используется для поиска наилучших технических решений для достижения указанных требований. Решаются задачи анализа эффективности работы конкретных технических элементов приёмных и передающих трактов, использования антенн с заданной геометрией и системой управления, ЗС с заданными режимами модуляции и пр. Это позволит поводить сравнение компоновок РЛС на базе готовых модулей, производство которых освоено, а также исследовать вопросы необходимости разработки новых образцов указанной техники. На структурном уровне РЛС представлена набором компонентов — программных модулей и связей между ними. Модель РЛС на структурном уровне выполненную в виде графа потоков данных, можно отображать, создавать и оперативной корректировать визуальными средствами редактора. Настройки режимов работы такой модели возможны путём задания фактических параметров работы её элементов, а также путём глубокой перекомпоновки в редакторе. Также на этом уровне содержатся инструменты разработчика алгоритмов обработки радиолокационной информации, цифровой обработки сигналов и управления режимами работы РЛС.

Текущая реализация подсистемы имитационного моделирования строится по монолитной архитектуре. С учетом широкой кооперации задействованных соисполнителей и для обеспечения масштабируемости, открытости и многократного повторного использования разработанных имитационных моделей целесообразно рассмотреть вопрос перестроения подсистемы имитационного моделирования САПР РЛС на

основе существующего хорошо проработанного и апробированного стандарта, устанавливающего правила взаимодействия моделей и разработки программных интерфейсов. В качестве такового выбран стандарт IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) — стандарт архитектуры высокого уровня для моделирования и имитации, сокращенно — HLA. Актуальной на настоящий момент является версия стандарта IEEE 1516-2010.

Отмечаются и сложности такого перехода. Технология HLA непроста в изучении, а также «заточена» на максимальную автономность моделирующих агентов (федератов — в терминах HLA); первое обстоятельство ведет к значительным увеличениям трудозатрат на начальной стадии проекта (которые потенциально окупаются в будущем), второе — к некоторым принципиальным архитектурным ограничениям.

Ключевые слова: имитационное моделирование; дискретно-событийное имитационное моделирование; моделирование боевых действий; моделирование радиолокационных станций.

К ВОПРОСУ ПОСТРОЕНИЯ АГЕНТНОЙ МОДЕЛИ ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Волков Денис Владимирович

кандидат технических наук,
16 Центральный научно-исследовательский испытательный
ордена красной звезды институт имени маршала войск связи А.И.Белова,
г. Мытищи, Россия, denmarath@mail.ru

Саенко Игорь Борисович

доктор технических наук, профессор,
Военная академия связи имени Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия, ibsaen@mail.com

Шакуров Радик Шамилевич

кандидат технических наук,
16 Центральный научно-исследовательский испытательный
ордена красной звезды институт имени маршала войск связи А.И.Белова,
г. Мытищи, Россия, kolobrodov75@mail.ru

Уланов Андрей Вячеславович

кандидат технических наук,
16 Центральный научно-исследовательский испытательный
ордена красной звезды институт имени маршала войск связи А.И.Белова,
г. Мытищи, Россия, ulanov_a_v@mail.ru

В процессе создания сложных систем военного назначения возникают значительные трудности. Из-за уникальности систем и отсутствия аналогов нет достаточного опыта проведения работ по их проектированию. В связи с этим возникает необходимость в концептуальном моделировании создаваемых систем.

Под концептуальной моделью системы понимается абстрактная модель, содержащая описание преимущественно на качественном уровне принципов постро-

ния, структуры системы (ее элементов, их взаимосвязей, этапов структурного синтеза), анализ ее существенных свойств на предмет соответствия требованиям, а также основные вопросы организации управления ею в процессе функционирования.

В качестве исходного материала для выбора показателей качества функционирования следует рассмотреть показатели, уже апробированные и используемые для оценки различных сетей (информационно-вычислительных, передачи данных и др.). Поскольку система связи специального назначения как объект оптимизации представляет собой сложную систему, характеризуемую многими параметрами, причем попытка улучшения одних характеристик может приводить и часто приводит к ухудшению других характеристик системы, выбор показателя оценки качества системы связи специального назначения затруднен.

Анализ современной системы связи специального назначения позволил сформулировать исходные данные, такие как: типовой и количественный состав согласно постановке задачи; местоположения пунктов управления согласно обстановке, маршруты до всех пунктов управления; процесс оформления заявки на обслуживание, заказа запчастей и т.п.;

Ограничения и допущения:

– среднесуточные потери определяются установленными нормативами;

– поток эксплуатационных отказов в течении суток простейший;

– время восстановления является случайной величиной, распределенной по экспоненциальному закону;

– каждый пункт управления отправляет запрос одинаковой формы на обслуживание, ремонт и т.п.;

Имитационное моделирование является одним из мощных инструментов для анализа и синтеза, который используют специалисты при исследовании и проектировании сложных систем.

Общеизвестно, что правильно поставленный натурный эксперимент, т.е. исследование свойств объекта на самом объекте, максимально информативен. Оказывается, что эксперимент с компьютерной имитационной моделью вполне конкурентоспособен с натурным экспериментом. Не говоря о том, что натурный эксперимент в ряде случаев вообще невозможен или нецелесообразен, эксперимент с имитационной моделью может быть приемлемо информативным и выполнен значительно быстрее и дешевле натурного.

Предлагаемый подход к построению модели технического обеспечения системы связи специального назначения на основе агентного моделирования, в отличие от известных подходов к построению имитационных моделей, позволяет исследовать систему «снизу-вверх». Взаимодействие агентов порождает новое поведение системы, учитывающее воздействие различных факторов. Разработанная модель предоставляет возможность оценивать качество функционирования системы связи специального назначения по качеству функционирования ее объектов, представленных в моделях в виде отдельных взаимодействующих агентов, и с учетом множества случайных факторов. Агентная модель технического обеспечения системы связи специального назначения является универсальной для систем, реализующих аналогичные функции и позволяет имитировать, задавать и изменять множество характеристик сети в широком диапазоне, а также определять коэффициент технической готовности этой системы.

Ключевые слова: имитационное моделирование; агентная модель; техническое обеспечение; система связи; коэффициент технической готовности.

К ВОПРОСУ О ФОРМИРОВАНИИ ПРОЕКЦИОННЫХ ДАННЫХ И РЕКОНСТРУКЦИИ ИЗОБРАЖЕНИЙ В РЕНТГЕНОВСКОЙ КОМПЬЮТЕРНОЙ ТОМОГРАФИИ

Курченко Александр Дмитриевич

*Военно-учебный научный центр «Военно-морская академия»
имени адмирала флота СССР Н.Г.Кузнецова,
г. Санкт-Петербург, Россия, nukdan@mail.ru*

С целью повышения эффективности методов реконструкции изображений, полученных в результате проведения процедуры формирования проекционных данных, используемых в проведении компьютерной томографии, предлагается техническое решение, решающее обратную задачу, основанную на аналитическом описании реконструкции изображения и его дискретном подходе, обеспечивающем параллельную и веерную геометрию сканирования поверхности исследуемого объекта. Практическая направленность данного технического решения в силу своих уникальных свойств, основанных на визуализации плотности в каждой точке исследуемого объекта, находит все большее применение в современных радиотехнических системах и комплексах, особенно в задачах реконструкции изображений, полученных при исследовании радиолокационной обстановки. Однако на качество изображения, полученного в результате реконструкции влияют факторы, снижающие качество проекционных данных (погрешности, шумы), по которым проводится их реконструкция. А сам алгоритм реконструкции, должен быть устойчив к погрешностям и шумам проекционных данных. В связи с этим предлагается рассмотреть техническое решение, позволяющее усовершенствовать алгоритм реконструкции томографического изображения с целью улучшения качества проекционных данных и изображений и повышающие устойчивость алгоритмов реконструкции. Для оценки эффективности предлагаемого технического решения, направленного на реконструкцию изображений, дополнительно проводятся экспериментальные исследования методов регуляризации в условиях влияния сложной помеховой обстановки, в состав которых входят: методы, основанные на усечении области частот Фурье с использованием сворачивающих функций (временных окон) и методов, основанных на регуляризации Тихонова.

Ключевые слова: радон; рентгеновские лучи; дискретный подход; пиксель; гауссовский шум.

КОРРЕЛЯЦИОННЫЙ АНАЛИЗ МУЗЫКАЛЬНЫХ ПРОИЗВЕДЕНИЙ С НИЗКОЧАСТОТНЫМИ ФЛУКТУАЦИЯМИ МИКРОВОЛНОВОГО ИЗЛУЧЕНИЯ СОЛНЦА НА ОСНОВЕ ВЕЙВЛЕТ ПРЕОБРАЗОВАНИЕ

Даровских Станислав Никифорович

доктор технических наук, доцент,
Южно-Уральский государственный университет,
г. Челябинск, Россия, darovskih.s@mail.ru.

Шоназаров Парвиз Махмадназарович

Южно-Уральский государственный университет,
г. Челябинск, Россия, shonazarov1991@gmail.com.

Махмадов Сино Анварович

Таджикский технический университет имени академика М.С.Осими,
г. Душанбе, Таджикистан, sino_205@mail.ru

На основе корреляционной обработки спектров музыкальных произведений известных композиторов доказывается высокий уровень их связи с низкочастотными флуктуациями микроволнового излучения Солнца, достигающего поверхности Земли. Выявленную закономерность можно интерпретировать так, что произведения известных музыкальных произведений есть не что иное как отражение в авторской обработке реальных природных процессов, к которым можно отнести флуктуации микроволнового излучения Солнца. Полученный результат может быть положен в основу обоснования необходимой процедуры определения тех или иных музыкальных произведений для их использования в лечебных целях. В этой статье представлен спектральный анализ музыкальных произведения с использованием вейвлет-преобразование. Программа, которая анализирует аудиосигналов в нашей работе разработана на языке программирование C#. Результате приведен преобразования нескольких музыкальных произведений низкочастотными флуктуациями микроволнового излучения Солнца. Вейвлет-преобразование — это математический инструмент, который обеспечивает постоянный добротность в спектральном анализе сигналов. Используется для спектрального анализа сигнала на ряду с преобразованием Фурье — классическим примером инструмента спектрального анализа. Название порождено из английского слова wavelet — что означает «короткая волна». Таким образом, он эффективно применен для анализа музыкальных сигналов, как частоты в музыкальном масштабе разделены логарифмически. Отмечены преимущества введенной корреляционной функции перед другими корреляционными функциями, в частности, возможности анализировать не только временные, но и частотные корреляции нестационарных сигналов. Для корреляционного анализа аудиосигналов программа разработано на языке программирование C#. Этот программа анализирует аудиосигналов на основе вейвлет-преобразование и показывает временная характеристика и спектрограмма аудиосигналов. Данном работе в мы коррелируем спектр аудиосигналов с низкочастотными флуктуациями микроволнового излучения Солнца. Разработка природоподобных технологий профилактики и лечения широкого спектра заболеваний человека — одно из перспективных направлений развития мировой системы здравоохранения. Сложность реализации указанного направления обусловлена неразрешенностью проблемы понимания механизма природной регуляции, обеспечивающего гомеостаз организма, определением основных его источников в ходе эволюции живой природы, а также причин его ослабления в современных

условиях. Важным фактором влияния на гомеостатические функции организма является акустический фон природного происхождения. Он представляет собой совокупность слабых механических возмущений различной физической природы, распространяющихся в упругой среде. Слышимые звуки являются важным источником информации для объектов живой природы, влияющих на их регуляторные функции. Эта закономерность нашла отражение в применении музыкальных произведений известных композиторов, в первую очередь, В. А. Моцарта для профилактики и лечении широкого спектра психосоматических заболеваний, развивающихся в организме как реакция на стресс. Близким по лечебному эффекту признаны григорианские песнопения, а также произведения И.-С. Баха, А. Вивальди, Г. Генделя, П. И. Чайковского, Ф. Шопена, Ф. Шуберта, Р. Шумана и др. Многочисленными исследованиями установлено, что под действием указанных музыкальных произведений осуществляется стимуляция иммунной системы, частично обусловленная необходимым синтезом дофамина для коррекции многих психических процессов [4–7]. Получение удовольствия от прослушивания музыки также связано с выработкой мозгом окситоцина, действующего как мягкий наркотик. Ряд исследователей связывают положительный эффект от прослушивания музыки с её согласованностью с частью высокочастотных биоритмов организма человека. Несмотря на большой объем информации о лечебном эффекте, указанной выше музыки при лечении психосоматических заболеваний человека, полного понимания того, что те или иные музыкальные произведения оказывают необходимое воздействие на организм, нет. Также не ясен эволюционный механизм высокой управляющей роли для организмов этих музыкальных произведений. Для разрешения указанных проблем необходимо проведение сравнительного спектрального анализа музыкальных произведений с реальными процессами природного происхождения, с которыми связана эволюция организмов и человека, в частности. Цель данной статьи состоит в оценке корреляционной связи спектров известных музыкальных произведений с низкочастотными флуктуациями микроволнового излучения Солнца, достигающего поверхности Земли, — основного источника формирования и эволюции регуляторных систем организмов. В данной работе проанализирован два новых подходов к анализу нестационарных, аудиосигналов. Первый подход основан на введение адаптивного вейвлета Морле, позволяющего изменять частотное и временное разрешения исследуемых сигналов с помощью данного метода. Второй метод связан с использованием корреляционный функции, которая двух представляет собой корреляция непрерывных вейвлетных преобразование двух сигналов, вычисленных как по частоте, так по времени. В статье представлены результаты анализа звуковых сигналов и корреляция с низкочастотными вариациями микроволновая излучения Солнца.

Ключевые слова: спектральный анализ; корреляционный анализ; вейвлет-преобразование; нестационарных сигналов; частотная корреляция; музыкальных произведений.

МЕТОД СНИЖЕНИЯ ВВОДИМОЙ ИЗБЫТОЧНОСТИ ПРИ КОНТРОЛЕ ЦЕЛОСТНОСТИ ДАННЫХ

Диченко Сергей Александрович

кандидат технических наук,
Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
г. Краснодар, Россия, dichenko.sa@yandex.ru

Финько Олег Анатольевич

доктор технических наук, профессор,
Краснодарское высшее военное училище имени генерала армии С.М. Штеменко,
г. Краснодар, Россия, ofinko@yandex.ru, http://www.mathnet.ru/rus/person40004

Рассматриваются системы хранения данных, предназначенные для хранения больших многомерных массивов информации, функционирующие в условиях деструктивных воздействий злоумышленника и среды. Одной из актуальнейших для подобных систем задач является организация безопасного хранения данных, а с учетом таких условий функционирования – обеспечение их целостности. Обеспечение целостности данных является сложной задачей, ввиду своей комплексности, так как включает в себя и восстановление, и контроль целостности данных. Одним из известных и широко используемых способов контроля целостности данных является применение криптографических методов, в частности, функции хэширования. Однако, несмотря на повсеместное применение хэш-функций, они крайне мало исследованы, а практические предложения по их применению весьма немногочисленны и характеризуются рядом недостатков, связанных, с необходимостью введения высокой избыточности контрольной информации. В условиях ограничения на существующий ресурс систем хранения данных это может привести к снижению вероятности выполнения задачи их функционирования или вообще к ее невыполнению. Предложен метод снижения вводимой избыточности при контроле целостности информации в системах хранения данных, основанный на применении криптографических хэш-функций, отличительной особенностью которого является использование правилах построения помехоустойчивых кодов, что позволяет снизить вводимую избыточность контрольной информации при заданном уровне защищенности данных. К тому же, применение разработанного метода обеспечивает процедуру контроля целостности данных новым свойством: возможностью осуществления контроля целостности не только данных, подлежащих защите, но и самих эталонных хэш-кодов. Получены расчетные данные требуемого объема вводимой избыточности при контроле целостности данных в существующих системах хранения при использовании разработанного метода.

Ключевые слова: система хранения данных; контроль целостности.

МОБИЛЬНОСТЬ СИСТЕМЫ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Сызранцев Алексей Геннадьевич

ФГУП «Центр МИР ИТ»,
г. Москва, России, sysrantsev18480@mail.ru

Исаева Анастасия Юрьевна

Московский технический университет связи и информатики,
г. Москва, России, nastja.1996@mail.ru

Федулов Андрей Владимирович

Московский технический университет связи и информатики,
г. Москва, России, andrej1964@mail.ru

Представлено понятие мобильности применительно к высокомобильному и стационарному компонентам системы связи специального назначения. Описаны этапы функционирования системы связи группировки специального назначения и ведения специальных оперативных действий, при которых к системе связи предъявляются наиболее высокие требования по мобильности. Обоснованы условия достижения высокой мобильности системы связи группировки специального назначения и выполнения предъявляемых требований. Оптимизация организационно-технической структуры системы связи и её элементов отмечена как одно из основных направлений достижения высокой мобильности, представлены методы и способы достижения этой оптимизации. Уделено особое внимание внешним факторам достижения высокой мобильности системы связи группировки специального назначения, зависящим не только от характеристики свойств системы связи группировки. Обосновано использование в качестве показателей мобильности временных характеристик, составляющих цикл управления системой связи группировки на различных этапах её функционирования. Даны особенности расчёта показателей мобильности стационарного и мобильного (полевого) компонентов системы связи группировки специального назначения, учитывающие особенности эксплуатации стационарных и полевых объектов системы связи группировки специального назначения.

Ключевые слова: группировка специального назначения; система связи группировки; орган управления; узел связи; свойства системы связи; мобильность.

НАУЧНО-ТЕХНИЧЕСКИЕ ПРЕДЛОЖЕНИЯ ПО ФОРМИРОВАНИЮ ИНФОРМАЦИОННЫХ РЕСУРСОВ КОМПЛЕКСОВ РАДИОМОНИТОРИНГА

Смирнов Андрей Александрович

кандидат технических наук,
Военная академия связи имени С.М. Буденного,
г. Санкт-Петербург, Россия, andrew_work@list.ru

Иванов Андрей Анатольевич

кандидат технических наук,
Военная академия связи имени С.М.Буденного,
г. Санкт-Петербург, Россия, a-a-iv@yandex.ru

Заика Павел Валентинович

Военная академия связи имени С.М. Буденного,
г. Санкт-Петербург, Россия, pashasever@mail.ru

Куликов Максим Владимирович

кандидат технических наук
Военная академия связи имени С.М.Буденного,
г. Санкт-Петербург, Россия, a-a-iv@yandex.ru

Наряду с развитием методов и средств обнаружения, измерения параметров радиоизлучений важной задачей совершенствования комплексов радиомониторинга является повышение эффективности процессов сбора данных от технических средств, их обработки и представления потребителям. Эффективность в данном случае оценивается системой показателей, характеризующих выполнение требований к результатам радиомониторинга — их своевременности, полноте и достоверности. В современных комплексах радиомониторинга реализация процессов сбора, обработки, представления и управления возлагается на информационно-управляющие системы. Проведенные исследования показали, что успешность их функционирования во многом определяется структурированностью, наполнением, актуальностью и интеллектуальностью информационных ресурсов, как совокупности хранилищ данных, участвующих в информационном процессе комплексов, а также алгоритмов их обработки. Научная проработка вопросов формирования информационных ресурсов, обоснования их структуры, порядка наполнения и обновления является перспективным направлением совершенствования комплексов радиомониторинга. В соответствии с назначением информационно-управляющих систем основными критериями оценки качества результатов радиомониторинга являются их полнота, достоверность и своевременность. Имея в виду, что целью функционирования комплекса радиомониторинга как системы является отслеживание радиоэлектронной обстановки в заданном районе, интегральным показателем его эффективности является расстояние между множествами, составляющими реальную радиоэлектронную обстановку и ее отображение, полученное в ходе радиомониторинга. Значение такого показателя представляет собой суммарное количество существенных ошибок в идентификации радиоэлектронных средств и измерении их параметров, а также количество радиоэлектронных средств, излучения которых измерены не были. Целью совершенствования системы радиомониторинга является минимизация этого показателя. Исходя из требований к результатам работы, структуре и функционалу информационно-управляющих систем разработаны модели

информационных ресурсов комплекса радиомониторинга, методика их наполнения и обновления. При разработке структурной модели информационных ресурсов комплексов радиомониторинга было выявлено следующее: структура информационных ресурсов, используемых операторами технических средств, информационно-управляющих систем комплексов, ситуационных центров радиомониторинга является одинаковой и состоит из баз данных результатов обработки информации, эталонных признаковых описаний объектов радиомониторинга, алгоритмов, процедур обработки данных радиомониторинга, фактографического информационного ресурса и исходных данных для обработки; ресурсы различных уровней отличаются наполнением (на практике к тому же и исполнением), при этом выходные данные ресурса нижележащего уровня являются исходными для вышестоящего уровня; взаимодействие элементов информационного ресурса внутри одного уровня и по иерархии подчинения обеспечивается алгоритмами, реализующими конкретные бизнес-политики обработки данных, управления, лежащие в основе соответствующих сервисов. Наполнение хранилищ с данными радиомониторинга и результатами их обработки осуществляется во время функционирования комплекса в процессе сбора и обработки данных, данные в них относятся к переменной информации и подвержены интенсивному старению. В отличие от них базы справочных данных, признаковых описаний и алгоритмы, процедуры обработки разрабатываются заранее и долгое время остаются актуальными. Учет актуальности, степени доверия к используемым в обработке данным лежит в основе выполнения требования к достоверности результатов радиомониторинга. Поэтому для определения периодичности обновления ресурсов с переменной и условно-постоянной информацией была разработана методика, основанная на экспоненциальном законе старения информации. Достоверность сделанных предположений о законе старения подтверждается множеством специальных исследований, а также результатами проведенного имитационного моделирования. Наиболее трудоемкой задачей, требующей научного обоснования, явилось определение состава и разработка методики наполнения фактографического информационного ресурса, обеспечивающего представление справочной информации по вопросам предметной области радиомониторинга в условиях автономного функционирования комплекса без подключения к глобальной информационной сети. Наполнение осуществляется на этапе подготовки комплекса к применению с использованием методов разведочного поиска и тематического моделирования. В отличие от классических методов, использующих для выявления тем и терминов коллекцию документов, предложено в качестве набора терминов на вход алгоритмов поиска подавать онтологию предметной области радиомониторинга, а при размещении результатов поиска документов в фактографическом информационном ресурсе тематически размечать их по аналогии с Semantic Web идентификаторами концептов онтологии и темами в виде названий экземпляров ее классов. В целях практической реализации представленных научных разработок по формированию информационных ресурсов комплексов радиомониторинга предлагается: 1. Ввиду высокой интенсивности поступления данных от технических средств радиомониторинга хранилище данных радиомониторинга организовать на основе NoSQL базы данных. Это позволит при систематизации данных эффективно и с минимальными затратами времени на процессы обращения к памяти применить технологии обработки больших данных, например, Map Reduce; 2. В качестве структуры данных фактографического информационного ресурса применять онтологию предметной области радиомониторинга, которая является основой схемы данных соответствующего хранилища (например, схемы данных индекса Elastic Search). Применение онтологии на этапе подготовки комплекса к применению позволит осуществить информационный

поиск в задаваемой онтологией предметной области с применением технологии тематического моделирования. Результаты тематического моделирования используются для автоматического тегирования документов фактографического информационного ресурса. В соответствии со структурой онтологии в индекс поисковой системы добавляются документы, составляющие информационный ресурс. Поисковая система обеспечивает выполнение поиска по документам ресурса с учетом морфологии и геопривязки на основе запросов из строки поиска; 3. Представление и хранение признакового описания радиоэлектронных средств и объектов радиомониторинга, результатов радиомониторинга реализовать с использованием объектно-реляционной системы управления базами данных (например, PostgreSQL), дополненной средствами хранения и обработки геопространственных данных (например, PostGIS); 4. Реализацию функционирования информационных сервисов, доступ к различным информационным ресурсам осуществлять с использованием одной из сервис-ориентированных технологий, например, интеграционной сервисной шины (Enterprise Service Bus). С точки зрения модели взаимодействия открытых систем она функционирует на прикладном уровне. При этом технология интегрированной сервисной шины предоставляет приложениям возможность функционировать через единую точку доступа к ресурсам, находящимся в информационно-коммуникационной сети. Основу реализации функций подсистем сбора данных от различных средств в технологии интеграционной сервисной шины осуществляют агент сообщений и шлюзы (программные модули, обеспечивающие взаимодействие с приложениями в том формате, который для них приемлем). Они представляют информацию от интегрируемых элементов (средств радиомониторинга, других подсистем комплексов радиомониторинга) в унифицированном формате интеграционной сервисной шины, воспринимаемом агентом сообщений. Представленные научно-технические предложения по формированию информационных ресурсов комплексов радиомониторинга показывают реализуемость разработанных ранее моделей их формирования, методик наполнения и обновления. Примененные программные решения не являются единственно возможными и были выбраны в качестве наиболее доступных программных средств с открытым исходным кодом среди прочих средств, удовлетворяющих рассмотренным требованиям.

Ключевые слова: информационные ресурсы; радиомониторинг; обработка данных радиомониторинга; интеграционная сервисная шина; информационно-управляющая система.

ОБРАБОТКА ИНФОРМАЦИИ В АСУ НА ОСНОВЕ УЛЬТРАЗВУКОВЫХ ПРИЕМО-ПЕРЕДАЮЩИХ УСТРОЙСТВ

Саидов Бехруз Бадридинович

Южно-Уральский государственный университет
г. Челябинск, Россия;
Таджикский технический университет имени М.С. Осими,
г. Душанбе, Таджикистан, matem.1994@mail.ru

Тележкин Владимир Федорович

доктор технических наук, профессор,
Южно-Уральский государственный университет
г. Челябинск, Россия, telezhkinvf@susu.ru

В современных автоматизированных системах управления (АСУ), в том числе и специального назначения, применяются методы обработки информации, широко использующие цифровые технологии и обмен данными по сети между разными сервисами. В АСУ также предполагаются совместные усилия группы (рабочей группы в сети) сотрудников для решения возникающих проблемы, обмена мнениями во время обсуждения в сети любого вопроса в режиме реального времени (телеконференция), оперативного обмена материалами через электронную почту, электронные доски объявлений и т. д. Для таких систем, охватывающих работу предприятия (и АСУ) в целом, используется термин «корпоративные автоматизированные системы управления процессами». Такие системы характеризуются использованием клиент-серверных технологий, включая подключение удаленных пользователей через глобальный (облачный) Интернет, а также использование физической среды и методов формирования сигналов для передачи данных. Все сигналы по способу представления делятся на четыре группы: аналоговые - описываются функциями, непрерывными во времени; дискретный - прерывается во времени с шагом, заданным выборкой; квантованные - имеют набор конечных уровней (обычно по амплитуде) цифровых — комбинацию свойств дискретных и квантованных сигналов. В зависимости от параметра несущей, который используется для кодирования (декодирования) информации, процесс называется амплитудной, частотной или фазовой модуляцией. Модуляция — это процесс изменения одного или нескольких параметров высокочастотной несущей волны согласно закону низкочастотного информационного сигнала (сообщения). В результате модуляции спектр низкочастотного управляющего сигнала передается в высокочастотную область. Это позволяет организации эфирного вещания настраивать работу всех приемопередатчиков на разных частотах, чтобы они не мешали друг другу. Актуальной научной задачей является повышение эффективности информационного обеспечения АСУ с помощью систем беспроводной связи на основе ультразвуковых технология передачи сигналов, включающих в себя модуль передачи и приемный модуль. Модуль передачи принимает входные сигналы от беспроводного устройства, модифицирует принятые входные сигналы таким образом, что преобразует каждый принятый входной сигнал в соответствующий ультразвуковой сигнал и беспроводным образом передает каждый упомянутый ультразвуковой сигнал через ультразвуковой канал. Приемный модуль принимает переданные ультразвуковые сигналы, восстанавливает соответствующие входные сигналы и позволяет выводить каждый соответствующий входной сигнал через одно или несколько выходных устройств. Модификация входных сигналов может включать

вейвлетное сжатие (общее название класса методов кодирования), кодирование и модуляцию входных сигналов. Входные сигналы могут быть речевыми аудио сигналами, позволяющими использовать систему поддержки телефонных звонков путем обеспечения возможности ультразвуковой связи, например, между беспроводной гарнитурой и мобильным телефоном. Модули передачи и приема могут быть связаны с беспроводной гарнитурой и мобильным телефоном для обеспечения ультразвуковой связи и, при необходимости, радиочастотной связи между ними. Вейвлет-преобразование — это преобразование, использующее функции, локализованные как в реальном, так и в пространстве Фурье. В основном оно делится на два типа. Один тип вейвлет-преобразования легко обратим. То есть, исходный сигнал может быть восстановлен после его преобразования. Пример: сжатие и очистка изображения. В этом случае: вейвлет-преобразование изображения вычисляется; представление вейвлета изменяется соответствующим образом; затем вейвлет-преобразование переворачивается для получения нового изображения. Второй тип вейвлет-преобразования предназначен для анализа сигналов. Пример: выявление обработка ультразвуковой сигналов. В этом случае модифицировать форму исходного сигнала не требуется. Так что Вейвлет-преобразование не нужно менять на противоположный. Но этот процесс требует много времени на вычисления. На основе ортогональности Вейвлет-преобразование можно разделить на две части. Одним из них является непрерывное вейвлет-преобразование или не избыточный вейвлет-преобразование, а вторым является дискретное вейвлет-преобразование или избыточное вейвлет-преобразование. Непрерывное вейвлет-преобразование возвращает массив на одно измерение больше входных данных. Оно в основном обеспечивает теоретическое направление для обработки ультразвуковой сигнала, тогда как дискретное вейвлет-преобразование осуществимо для практических ультразвуковых систем из-за быстрого времени вычисления и, таким образом, является предпочтительным. Дискретных вейвлет-преобразований возвращает вектор данных той же длины, что и входные данные. Он разлагается на набор вейвлетов, то есть функций, которые ортогональны его трансляциям и масштабированию. Следовательно, можно разложить такой сигнал на такое же или меньшее число спектра вейвлет-коэффициентов, как и количество точек данных сигнала. Такой вейвлет-спектр хорош для обработки и сжатия ультразвуковой сигналов. Таким образом, вейвлет-преобразование представляет собой бесконечный набор различных преобразований в зависимости от оценочной функции, используемой для ее вычисления. Информация о времени и частоте может быть получена одновременно с помощью вейвлет-преобразования. Целью данной работы является постановка задачи обработка ультразвуковых сигналов в приемо-передающей системе на основе вейвлет-преобразования.

Ключевые слова: обработки информации; ультразвуковой сигнал; вейвлет-преобразование.

ОПТИМИЗАЦИЯ ПРОЦЕССА РАСПРЕДЕЛЕНИЯ РЕСУРСОВ В ГЕТЕРОГЕННОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ

Минайчев Артем Андреевич

кандидат технических наук,
Академия федеральной службы охраны Российской Федерации,
г. Орёл, Россия, minaychev.artem@mail.ru

Полунин Александр Александрович

Академия федеральной службы охраны Российской Федерации,
г. Орёл, Россия, polunin2002@mail.ru

Рожкова Татьяна Сергеевна

Академия федеральной службы охраны Российской Федерации,
г. Орёл, Россия, rozhkova_tatyana92@mail.ru

В наши дни применение мобильных вычислительных устройств становится все более повсеместным. Однако, их возможности ограничены вычислительными ресурсами и энергоемкостью аккумулятора. На сегодняшний день широко применяется перенаправление сложных и ресурсоемких задач в удаленные облачные сервисы. Но при возрастании количества подобных задач увеличивается задержка передачи данных в сети, а также расход энергии при их передаче на большие расстояния. В связи с этим, в работе предлагается использование незадействованных вычислительных ресурсов мобильных устройств, находящихся в непосредственной близости, без передачи выполнения задач в удаленное облако.

В работе проводится обоснование и выбор модели распределения рабочей нагрузки в распределенной вычислительной системе, ставится задача – минимизировать среднее время отклика всех пользователей, с учетом разных скоростей поступления рабочей нагрузки на разные узлы системы. Рассмотрен общий случай распределения ресурсов на примере двух вычислительных узлов, расширение его до корпоративной вычислительной сети, а также частый случай с участием координатора распределения вычислительных ресурсов. Поставлена задача оптимизации для одноузловой вычислительной сети и задача оптимизации при кооперативных вычислениях. Произведен анализ существующих традиционных подходов и их сравнение в рамках поставленной задачи. В силу их несостоятельности для рассматриваемого объекта исследования предлагается новая распределенная структура оптимизации, основанная на разложении исходной задачи на ряд подзадач, каждая из которых может быть решена любым узлом системы с использованием ее частной информации.

Оптимизация решения подзадач всех узлов координируется через координатора пересылки рабочей нагрузки, который может быть установлен в качестве облачного дата-центра. В качестве координатора ресурсов может выступать сервер или высокопроизводительный кластер. Разработанная модель позволяет перенести часть вычислительных задач на отдельный сервер, что способствует распределению рабочей нагрузки мобильных устройств и снижает потребление энергии их аккумулятора.

Ключевые слова: распределенная вычислительная система; вычислительные ресурсы; координатор распределения ресурсов; интернет вещей; беспроводные сенсорные сети; туманные вычисления.

ОЦЕНКА КАЧЕСТВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ НА ОСНОВЕ ОДНОСТУПЕНЧАТОГО ПЛАНА ИСПЫТАНИЙ

Репин Сергей Иванович

доктор технических наук, профессор,
Научно-производственное объединение
«Русские базовые информационные технологии»,
г. Тверь, Россия, s.repin@rusbitech.ru

С теоретико-вероятностной точки зрения надежность программного обеспечения автоматизированных систем относится к наиболее важным и системным показателям качества. Особенность системности надежности программного обеспечения автоматизированных систем заключается в том, что она определяется не только надежностью отдельных компонентов и подсистем, но и взаимным влиянием на нее других показателей качества. Поскольку программное обеспечение в процессе эксплуатации не изнашивается, его поломка и ремонт в общепринятом смысле не производится, то надежность программного обеспечения имеет смысл характеризовать только с точки зрения безотказности его функционирования и возможности восстановления функционирования после отказов вызванных проявлениями ошибок. При оценке надежности программного обеспечения автоматизированных систем не существует понятия выборка, отказы не зависят от времени и отказы не имеют случайной природы. В тоже время при оценке показателей надежности программного обеспечения автоматизированных систем следует учитывать и различать такие понятия как ошибка, отказ и сбой. На основе введенной размерности временных зон перерыва нормальной выдачи информации и потери работоспособности автоматизированных систем предложены критерии для выявления ошибок, сбоев и отказов в программном обеспечении. Анализ семантики показателей надежности программного обеспечения автоматизированных систем показал, что основными компонентами надежности их программного обеспечения следует считать стабильность, устойчивость и восстанавливаемость. На основе выбранной единой системы показателей для аппаратно-программных комплексов предложен методический подход и разработан алгоритм оценки надежности программного обеспечения с использованием одноступенчатого плана испытаний. Предложенный алгоритм имеет практическую направленность решения задач оценивания качества программного обеспечения объектов самого широкого назначения, подкреплен действующими нормативными документами и направлен на обеспечение требуемой достоверности оценивания показателей надежности автоматизированных систем на этапе их создания.

Ключевые слова: инфокоммуникационные технологии, качество программного обеспечения, показатели надежности, ошибка, отказ, сбой.

ПОВЫШЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ БЕСПРОВОДНЫХ ЛИНИЙ СВЯЗИ НА ОСНОВЕ ПРИМЕНЕНИЯ МИКРОПОЛОСКОВЫХ АНТЕНН ТЕХНОЛОГИИ MIMO 2×2

Чуян Виктория Александровна

ФГУП «Центр МИР ИТ»,
г. Москва, России, viktoriaprokofeva471@gmail.com

Кожанова Кристина Евгеньевна

Московский технический университет связи и информатики,
г. Москва, России, su7b1986@mail.ru

Представлено обоснование необходимости совершенствования антенного оборудования, работающего в диапазоне частот 1850–1990 МГц. Рассмотрены возможные варианты разработки и реализации микрополосковой антенны с использованием технологии MIMO (Multi Input Multi Output). Обоснована схема реализации антенны, проведён и представлен расчёт характеристик излучения антенны. Разработана и описана геометрия полосковой антенны прямоугольной формы и точка подключения питания для обеспечения максимального согласования. Антенна разработана в программном комплексе Altair FEKO. Антенна с использованием ортогональной поляризации, которая дает лучший результат с точки зрения возвратных потерь и взаимной связи. Разработанная и описанная антенна технологии MIMO 2×2 обеспечивает наибольшую пропускную способность в беспроводных линиях связи по сравнению с использованием других технологий. Антенна рассчитана на рабочую частоту 1850–1990 МГц. Предложены возможные размеры антенны и её применения в терминальных устройствах потребителей услуг связи.

Ключевые слова: MIMO (Multi Input Multi Output); микрополосковая антенна; многоканальная система; ортогональная поляризация, взаимная связь; магнитные токи; излучатель.

ПОКАЗАТЕЛЬ КАЧЕСТВА ГРАФИЧЕСКОГО ИНТЕРФЕЙСА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА СВЯЗИ

Федорова Светлана Викторовна

Военная академии связи имени С.М. Буденного,
г. Санкт-Петербург, Россия, svetafedorov@mail.ru

Взаимодействие оператора с программно-аппаратным комплексом связи осуществляется через пользовательский интерфейс, включающий аппаратную и программную составляющую. Проведено достаточное количество исследований, доказывающих влияние пользовательского интерфейса на результат трудовой деятельности операторов. Так «плохо» спроектированный пользовательский интерфейс может стать источником стресса и психологического дискомфорта оператора,

которые приведут к уменьшению производительности оператора и возрастанию количества ошибок в его работе. Проектирование и разработка графического пользовательского интерфейса, как правило, возложены на специалиста осуществляющего проектирование и разработку всего программного обеспечения образца техники. Такой специалист обычно не обладает знаниями в области эргономики программного обеспечения и «пишет» интерфейс лишь с учетом выполняемых техникой функций, заданных в тактико-техническом задании заказчиком и собственными субъективными представлениями о понятности и удобстве интерфейса. На сегодняшний день существует достаточно много методик оценки эргономичности интерфейса, но они используются разрозненно, в зависимости от принятых у разработчиков способов его разработки и методов оценки. Каждый из этих методов обладает рядом недостатков и не позволяет с достаточной полнотой дать оценку по всем эргономическим параметрам интерфейса.

В связи с этим разработаны конкретные предложения формального математического описания интерфейса и его элемента. Предложен вариант оценки эргономичности интерфейса с помощью многокритериального показателя качества. Математическое описание интерфейса, как и большинства сложных систем, предложено определять с помощью математического описания элементов, входящих в его состав, которое в свою очередь осуществить с помощью основных его параметров. Предложен перечень этих параметров. С помощью математического описания элементов графического пользовательского интерфейса, параметров и их изменений, можно провести сравнительную характеристику показателей качества интерфейса и определить с какими параметрами элементов и их составом интерфейс будет обладать более высоким показателем качества. Несмотря на концептуальную простоту, предложенный подход дает общий способ оценки качества графического пользовательского интерфейса.

Ключевые слова: пользовательский интерфейс; графический интерфейс; качество интерфейса; показатель качества; эргономическая оценка интерфейса.

ПРИМЕНЕНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИИ ДЛЯ ПОСТРОЕНИЯ КРИТИЧЕСКИ ВАЖНЫХ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ: КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ

Фабияновский Игорь Николаевич

*Военная академия связи имени Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия, Fabik-spb@yandex.ru*

Николаев Владимир Витальевич

*Военная академия связи имени Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия, valeron12.1366@gmail.com*

Саенко Игорь Борисович

*доктор технических наук, профессор,
Военная академия связи имени Маршала Советского Союза С.М. Буденного,
г. Санкт-Петербург, Россия, ibsaen@mail.ru*

Современным подходом к созданию критически важных распределенных информационных систем (КВРИС) является направление, основанное не на постоянной модернизации существующей системы, а на использовании современных информационных технологий. Это позволяет повысить эффективность информационного взаимодействия органов управления (ОУ) в крупных организациях, без существенных затрат. На сегодняшний день постоянное нарастание объема и разнообразия информации, циркулирующей в системе управления, требует постоянного увеличения пропускной способности каналов для обеспечения гибкого и оперативного реагирования на изменения обстановки в режиме реального времени. В таких условиях сокращение времени на сбор информационных ресурсов (ИР) от ОУ, описывающих изменение их состояния и состояния внешний окружающей среды в режиме реального времени, напрямую зависит от структуры управления, объема ИР и их доступности. Такие системы автоматизации должны иметь доступ к большому объему оперативно обновляемой информации, быть способными своевременно ее обрабатывать и наглядно отображать результаты. На сегодняшний день такая задача является весьма сложной и актуальной. В связи с этим предлагается пересмотреть существующие взгляды на информационный обмен между органами управления, участвующими в решении специальных задач.

Среди систем, автоматизирующие такие информационные процессы, значительное место занимают транзакционные системы. Их также называют учетно-отчетные, информационно-справочные системы. Такие системы работают с небольшими по размеру транзакциями, идущими большим потоком, с минимальным временем доведения до УО. Особенностью таких систем является то, что информация, циркулирующая в такой системе, идет снизу вверх по системе управления и инициирует управленческие воздействия, позволяя выбирать тот или иной способ, имея при этом форму неструктурированных данных (НД).

Проведенный анализ предметных областей, специализирующихся на отраслевых решениях с массовыми транзакциями, показал довольно низкую оперативность обработки НД в КВРИС. Связано это с хранением множеств ИР, различных по объему и времени их передачи, увеличением количества пользователей, доработкой и расширением функциональных возможностей системы и т.д.

Ввиду большого разнообразия современных информационных технологий проведен их сравнительный анализ, по результатам которого можно сделать вывод, что блокчейн-технология обладает более высокой оперативностью сбора ИР при ее децентрализации, а также имеет более высокую доступность к хранящимся ИР. Достигается это за счет дублирования специальным образом полной копии реестра в каждой локальной БД.

Рассмотрен общий алгоритм функционирования системы распределенного реестра применяемый в блокчейн-технологии, результатом которой является распределенный реестр. Приведен пример ее работы в организации, из рассмотрения которого следует вывод о том, что блокчейн-технология позволяет повысить производительность КВРИС, обеспечивая при этом необходимую безопасность хранения ИР. Данное обстоятельство обусловлено существенным влиянием производительности на другие свойства КВРИС, а безопасность является противоположным свойством для производительности. Возможные различные варианты соотношений производительности и безопасности КВРИС при помощи соответствующих им критериев, которые выражаются через коэффициент своевременности и коэффициент доступности.

Таким образом, требуется разработка инструментария, учитывающая данные свойства и критерии. Разрабатываемый инструментарий должен обеспечить управление информационных ресурсов в КВРИС в реальном масштабе времени по единым принципам, вне зависимости от технологических особенностей оборудования и систем связи различных типов. Построение КВРИС на основе применения блокчейн-технологии позволит существенно повысить ее производительность, сохраняя при этом требуемую безопасность хранимых ИР.

Ключевые слова: распределенная информационная система; блокчейн; информационная технология; информационный ресурс.

ПРОГРАММНЫЙ КОМПЛЕКС МОДЕЛИРОВАНИЯ ПАКЕТНЫХ РАДИОСЕТЕЙ КВ-ДИАПАЗОНА

Дорогов Александр Юрьевич

доктор технических наук, доцент,
публичное акционерное общество «Информационные телекоммуникационные технологии»,
г. Санкт-Петербург, Россия, vaksa2006@yandex.ru

Яшин Александр Иванович[2]

доктор технических наук, профессор,
публичное акционерное общество «Информационные телекоммуникационные технологии»,
г. Санкт-Петербург, Россия, vaksa2006@yandex.ru

Ионосферная радиосвязь в КВ диапазоне (3÷30 мГц) является экономически эффективной средой для многих видов телекоммуникационных услуг, требующих передачи данных за пределы прямой видимости. Для Российской Федерации высокона-

дёжная сеть КВ-диапазона масштаба страны представляется недорогой альтернативой спутниковым системам связи при предоставлении телекоммуникационных услуг службам МЧС, РЖД, силовым ведомствам, а также региональным администрациям и многочисленным хозяйственно-экономическим структурам.

Для КВ-диапазона определяющим фактором распространения радиоволн является наличие околоземной ионосферы. Структура и свойства ионосферы существенно изменяются с высотой. Процессы, протекающие в ионосфере, тесно связаны с волновым и корпускулярным излучением Солнца, с процессами в магнитосфере, вариациями магнитного поля Земли, с движением верхней атмосферы и т.д.. Этим обусловлена сильная изменчивость свойств ионосферы от времени суток, времени года, циклов солнечной активности, а также в зависимости от высоты и наличия отражающего слоя, географической широты и долготы приёмника и передатчика.

Сложность и постоянная изменчивость структуры ионосферы, наличие множества факторов оказывающих влияние на распространения радиоволн в такой среде, а также сложная топология сетей связи приводят к необходимости компьютерного моделирования передачи данных в сетях КВ-диапазона. Длительную историческую традицию имеет подход, основанный на использовании ионосферных моделей, как правило, из класса статистических среди которых наиболее распространённой и обоснованной в настоящее время является модель IRI (International Reference Ionosphere. IRI – это международный проект, спонсируемый Комитетом по космическим исследованиям (COSPAR) и Международным союзом радиовещания (URSI). Эти организации создали рабочую группу, которую вошли представители различных стран, в том числе и из России. Модель ионосферы впервые была предложена в конце 60-х на основе всех доступных источников данных. Выпущено несколько версий модели, в настоящее время действует модель IRI-2016. Для данного местоположения, времени и даты IRI предоставляет медианные значения электронной плотности, электронной температуры, температуры ионов, состава ионов в диапазоне ионосферных высот, критические частоты распространения радиоволн КВ-диапазона и другие данные. Модель поддержана программными средствами открытого доступа, реализованными на языках Fortran, Python, Matlab. К сожалению, модель не охватывает полностью спектр задач прогнозного моделирования распространения радиоволн на протяжённых трассах. В частности моделью не поддерживается расчёт уровней потерь на радиотрассах, влияние естественных и индустриальных помех на распространение сигнала, многолучевое распространение радиоволн, селективные замирания сигналов и другие характеристики, необходимые для проектирования КВ-радиосетей. Существует ряд рекомендательных моделей разработанных Международным Союзом Электросвязи (ITU) дополняющих модель IRI

В ITU разработана также комплексная математическая модель для прогнозирования рабочих характеристик ВЧ-линий, интегрирующая в себе набор частных моделей. Комплексная модель оформлена в виде рекомендации МСЭ-R P.533-13и программных средств для ОС Windows на языке Fortran . Модель позволяет производить расчёт характеристик КВ-радиолиний с протяжённостью до 9000 км (в режиме «Точка-точка») и радиозон покрытия (в режиме «Зона») с учётом уровней потерь на радиотрассах, влияние естественных и индустриальных помех на распространение сигнала, многолучевого распространение радиоволн. Программные средства доступны в виде исполняемых программ моделирующего комплекса и исходных кодов отдельных подпрограмм. В состав комплекса входит база данных антенн и редактор для изменения их характеристик. Комплексный характер модели позволяет минимизировать затраты на разработку дополнений.

Следует отметить, что исходные коды комплексной модели написаны на языке Fortran старой версии и поэтому требуют адаптации к современным компиляторам. Для отдельных подпрограмм представлен управляющий интерфейс, реализованный на основе устаревшей библиотеки ClearWin+. Исходные коды представляют собой набор подпрограмм и статических библиотек из программных модулей. Программный интерфейс к модулям не стандартизован. Указанные обстоятельства потребовали модификации исходного программного обеспечения и разработки собственного программного и пользовательского интерфейса для моделирующего комплекса. В новом варианте программный и пользовательский интерфейсы были реализованы средствами программной среды Matlab. Новый моделирующий комплекс использует структуру директориев исходного комплекса, и полностью совместим с ним по форматам хранения данных. Представленные модели дополняют разработанный ранее комплекс имитационного моделирования сетевых и транспортных протоколов пакетной радиосети. В статье представлены принципы построения моделирующего комплекса и результаты его применения для расчёта протяжённых радиолиний сети КВ-диапазона. Целью данной работы является постановка задачи имитационного моделирования КВ-радиосетей при изменяющихся условиях связи.

Ключевые слова: ионосфера, радиолиния, цифровой модем, радиозона, радиосеть, применимые частоты, отношение сигнал/шум, волновое расписание.

СПОСОБ КОНТРОЛЯ БЕЗОПАСНОСТИ В КОРПОРАТИВНОЙ СЕТИ MPLS НА ОСНОВЕ АНАЛИЗА ТРАФИКА

Бирюков Артем Сергеевич
Военная академия связи имени С. М. Буденного,
г. Санкт-Петербург, Россия, Biryukov-artem@list.ru

Вопросы защиты информации в компьютерных системах чаще всего разделяют две части: проблемы безопасности компьютера и проблемы безопасности сети.

К безопасности компьютера причисляют все вопросы защиты данных, сохраняемых и обрабатываемых компьютером, который считается изолированным устройством. Эти вопросы решаются средствами операционных систем и программ, например базы данных, серверы приложений и т.д., а так же собственными аппаратными средствами компьютера.

К проблемам безопасности сети причисляются все вопросы, проявляющиеся при сетевом взаимодействии устройств. Это, в первую очередь, предохранение данных во время их трансляции по линиям связи и предохранение от несанкционированного доступа в сеть сторонних лиц и приложений.

Несмотря на то, что проблемы безопасности компьютеров и сети тяжело разделить друг от друга, абсолютно бесспорно, что безопасность сети имеет свои отли-

чительные черты. Включенный в сеть компьютер не имеет возможности совершенно изолироваться от постороннего вмешательства. Он по определению обязан взаимодействовать с прочими устройствами, вероятно, даже размещёнными на значительном удалении от него. Таким образом, обеспечение безопасности сети – это проблема ещё более трудная. Кроме проблем, возникающих при наличии вероятности удаленного доступа к включенным в сеть компьютерам, в сетях встречается ещё один тип угроз – перехват и чтение данных, транслируемых внутри сети, а также вводу недостоверной информации. Значительная доля способов обеспечения сетевой безопасности сосредоточена на защите собственно от подобных типов угроз. Вопросы сетевой безопасности имеют огромное значение при создании компьютерной сети предприятия на основе общедоступных сетей (например, Интернет). Провайдеры доступа к ним нечасто озадачиваются защитой данных пользователей при их трансляции по своим линиям связи, оставляя проблемы по обеспечению доступности, целостности и конфиденциальности информации на пользователях. Целью данной работы является повышение оперативности контроля сети MPLS для обеспечения информационной безопасности.

Ключевые слова: сетевой контроль, анализ трафика, служебный и пользовательский трафик, кибербезоопасность, информационно-телекоммуникационные сети, цифровой поток.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИИЯ ВЫСОКОДИНАМИЧНЫХ АВТОМАТИЧЕСКИХ ТРАНСПОРТНЫХ СЕТЕЙ СВЯЗИ

Сызранцев Геннадий Валентинович

доктор военных наук, доцент,
ФГУП «Центр МИР ИТ», г. Москва, Россия, sysr9959@mail.ru

Мордвинцев Михаил Михайлович

Московский технический университет связи и информатики,
г. Москва, Россия, michael@mail.ru

Сызранцев Василий Сергеевич

отрытое акционерное общество «СУПЕРТЕЛ»,
г. Санкт-Петербург, Россия, sizrancev_vs@supertel.ru

Представлены обоснованные теоретические основы построения сложных организационно-технических систем применительно к автоматическим высокодинамичным системам управления связью (системам связи). Определены условия, при которых выполняется процесс управления связью в автоматических транспортных сетях связи. Процесс управления связью в интересах построения системы связи группировки специального назначения представлен по содержанию, организации и

процедурам осуществления управления. Обоснованы и представлены условия обеспечения автоматизации сетевых технологических процессов управления транспортными сетями связи и автоматического автономного функционирования сетей связи по заранее сформированным данным без оперативного вмешательства со стороны системы управления сетью связи. Обосновано применение оборудования технологии PDH для построения автоматических транспортных сетей связи высокодинамичных систем связи специального назначения. Определены требования для обеспечения автоматизации технологического управления сетью связи и непосредственного её функционирования по предназначению. Процесс управления связью рассмотрен с точки зрения технологии управления и представлен в виде трёх циклов и связей между ними: информационный, логико-мыслительный и вычислительный и организационный цикл. Определены требования к принимаемым решениям по связи для обеспечения эффективного функционирования системы связи. Обоснованы исходные данные, необходимые для обеспечения автоматизации технологического управления сетью связи и её функционирования в составе высокодинамичных систем связи специального назначения.

Ключевые слова: система управления связью; система связи; пункт управления связью, система сетевого технологического управления; автоматизация процессов технологического управления функционированием сети связи.

ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ НАЗЕМНОЙ ПАКЕТНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ ПРИ УПРАВЛЕНИИ КОСМИЧЕСКИМИ АППАРАТАМИ

Архангельский Алексей Алексеевич

кандидат технических наук, доцент,

Военно-космическая академия имени А.Ф.Можайского,
г. Санкт-Петербург, Россия, arhangelssky@yandex.ru

Топорков Николай Святославович

Военно-космическая академия имени А.Ф.Можайского,
г. Санкт-Петербург, Россия, k.toporkov@mail.ru

Процесс управления космическим аппаратом можно разделить на следующие элементы:

– получение информации о состоянии космического аппарата;

– введение управляющего воздействия;

–- получение информации о результатах управления космическим аппаратом;

– анализ полученной информации и выработка решения об управляющем воздействии (корректировке) состояния космического аппарата.

Реализация процессов управления космическими аппаратами входит в функции наземного автоматизированного комплекса управления, который включает в се-

бя центр управления полетом, наземные станции командно-измерительной системы и систему связи передачи данных.

Для формирования телеметрической информации на борту космического аппарата устанавливается специальная бортовая система контроля, которая осуществляет следующие действия:

– измерение параметров бортовых систем с использованием датчиков и преобразование результатов измерений в электрические сигналы;

– объединение сигналов с информацией о различных параметрах бортовых систем для передачи по радиоканалу.

Система информационно-телеметрического обеспечения производит прием телеметрической информации и телесигнализации, а также обработку и анализ ее для оценивания и прогнозирования технического состояния бортовых систем космического аппарата.

Телеметрическая информация имеет следующие особенности:

– большой объем и высокая интенсивность передачи информации;

– высокая частота опроса датчиков (50-100 измерений/с);

– разнородность измеряемой информации.

Наземная система связи передачи данных является важным элементом для процесса управления космическим аппаратом, поскольку входит в различные контуры управления. Далее рассматривается эффективность процесса функционирования наземного фрагмента сети, состоящего из локальной сети, подключенной к оптоволоконной системе передачи, по критерию соотношения количества основной и служебной информации.

В настоящее время уменьшились технологические различия между локальными и глобальными сетями, происходит объединение технологий процессов передачи информации, в локальных сетях используется коммуникационное оборудование: коммутаторы, маршрутизаторы, шлюзы, используются системы обработки мультимедийной информации (аудио и видео).

При анализе сложных технических систем удобно применять семиуровневую модель. В соответствии с семиуровневой моделью выделяются следующие уровни технических систем: физический (Physical); канальный (Data Link); сетевой (Network); транспортный (Transport); сеансовый (Session); уровень представления (Presentation); прикладной (Application). Локальная сеть объединяет нижние уровни семиуровневой модели от физического до транспортного.

Локальные сети подсоединяются к волоконно-оптической сети передачи данных. Параметры волоконно-оптической сети Fiber Distributed Data Interface – волоконно-оптический распределенный интерфейс данных определены стандартом American National Standard Institute. Сеть имеет топологию вида «двойное кольцо» со скоростью передачи 100 Мбит/с.

Для технических систем при исследовании их эффективности можно рассматривать следующие показатели:

– устойчивость функционирования;

– пропускная способность;

– оперативность;

– достоверности передачи информации;

– производительность системы и отдельных ее элементов,

– надежность.

При коммутации пакетов кроме абонентской информации передается служебная информация в виде заголовков. В данном случае критерием эффективности

является отношение количества переданной информации абонента к полному количеству переданной информации.

Комплексный критерий эффективности транспортной системы локальной сети и протокола определяется в мультипликативной форме.

Рассмотрена эффективность функционирования наземного фрагмента системы связи передачи данных для управления космическими аппаратами по критерию соотношения количества абонентской и служебной информации. Фрагмент сети состоит из локальной сети, подключенной к оптоволоконной системе передачи. При передаче через физический, канальный, сетевой, транспортный уровни интернет и по оптоволоконной сети коэффициент эффективности составляет $K_{лс} = 0,726$.

Это означает, что при номинальной производительности системы в 100 % абонентская информация составит не более 72,6 %, а остальная часть производительности системы используется для передачи служебной информации.

Ключевые слова: управление космическим аппаратом, телеметрическая информация, система связи передачи данных,

СЕКЦИЯ № 5

СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМ, КОМПЛЕКСОВ И СРЕДСТВ РАДИОСВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

ДВУХЛУЧЕВАЯ МОДЕЛЬ С ДИФФУЗНЫМ ЗАМИРАНИЕМ МОЩНОСТИ СИГНАЛА TWO-WAVE WITH DIFFUSE POWER FADING

Савищенко Николай Васильевич
доктор технических наук. профессор,
Военная академия связи имени С.М. Буденного,
г. Санкт-Петербург, snikaspb@mail.ru

Дырин Владимир Иванович
Военная академия связи имени С.М. Буденного,
г. Санкт-Петербург, dviumet@yandex.ru

Макаренко Владимир Петрович
Военная академия связи имени С.М. Буденного,
г. Санкт-Петербург, nsdiv@mail.ru

При обеспечении радиосвязи ионосферными волнами происходит случайный и временный характер изменения уровня принимаемого сигнала, называемый замираниями сигнала. Различают быстрые и медленные замирания сигнала. Быстрые замирания возникают из-за многолучевости принимаемого сигнала, лучи которого преодолели различное расстояние и число отражений от ионосферы и от земной поверхности. Неоднородность ионосферы, поляризация волн также приводит к замираниям сигнала. Для обеспечения достоверности и помехозащищенности информационного сигнала, при реализации, на этапе планировании и разработки процессов, необходимо особое внимание уделить вопросу передачи и приема информации по каналам связи.

Одной из основных задач математической теории связи является определение наиболее существенных характеристик системы передачи информации, к которым, в частности, относятся помехоустойчивость (вероятность ошибочного приема) и скорость передачи информации. Знание этих показателей позволяет определить, соответственно, качество и количество переданной информации. Можно выделить два основных типа каналов связи для которых чаще всего и определяются вероятности ошибок: детерминированный канал связи с аддитивным белым гауссовским шумом и канал связи с общими (частотно-неселективными) замираниями и аддитивным белым гауссовским шумом.

С целью вычисления вероятности ошибочного приема в канале связи с замираниями необходимо вычисление вероятности ошибочного приема сигнальных конструкций в канале связи с детерминированными параметрами и аддитивным белым гауссовским шумом и произвести выбор математической модели общих замираний, адекватной реальным процессам, протекающим в выбранном диапазоне волн. В настоящее время релеевские и райсовские замирания остаются наиболее используемой моделью. Ряд теоретических исследований показывает, что двухлучевая модель с диффузным замиранием мощности сигнала — более эффективно описывает замирания, что имеет очень важное значение для беспроводных систем и может подстраиваться под большое количество условий распространения лучей. Но эта гибкость достигается за счет большей сложности математического аппарата, из-за чего ее плотность распределения вероятности и кумулятивная функция распределения выражаются в интегральной форме либо в виде бесконечных рядов.

Ключевые слова: TWDP; замирания; помехоустойчивость; плотность распределения вероятности; многолучевая модель.

О МЕТОДОЛОГИИ УЧЁТА ЭФФЕКТА АСИММЕТРИИ ВРЕМЕНИ В ЗАДАЧАХ ОЦЕНКИ ПОКАЗАТЕЛЕЙ ДОЛГОВЕЧНОСТИ АСУ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Острейковский Владислав Алексеевич

доктор технических наук, профессор,
Сургутский государственный университет,
г. Сургут, Россия, ova@ivi.surgu.ru

Шевченко Елена Николаевна

кандидат физико-математических наук., доцент,
Сургутский государственный университет,
г. Сургут, Россия, elenan_27@mail.ru

Волков Александр Владиславович

Сургутский государственный университет,
г. Сургут, Россия, volk_234@mail.ru

1. Необратимость — объективная форма существования и устойчивых флуктуирующих динамических систем и играет важную конструктивную роль в процессах даже в совершенно различных областях науки, начиная с биологии и заканчивая космологией.

2. Необратимые процессы имеют свои закономерности на трех уровнях описания систем: субмикроскопическом, микроскопическом и макроскопическом. В конечном итоге такие микроскопические процессы как химические реакции, диффузия, адсорбция, распад твердых растворов, изменение механических, электрических и

магнитных свойств твердых тел и другие являются причиной более сложных деградационных макропроцессов: коррозия, эрозия, износ, ползучесть, усталость, деформации и другие. Причём такого рода необратимые процессы развиваются под воздействием комплекса эксплуатационных факторов в СФСС: динамические и статические механические нагрузки, термогидравлические и тепловые удары, перенос и осаждение продуктов коррозии, примесей и т.д. Поэтому необратимые процессы приводят к глубоким изменениям на самом фундаментальном уровне описания природы - на уровне пространственно-временного континуума.

3. Энтропийное время всегда направлено в одну сторону и не совпадает с ходом времени, отсчитываемый по обычным часам, и поэтому всегда эволюционирует в модусах «прошлое-настоящее-будущее», причём существует множество типов эволюции времени.

4. С точки зрения решения динамических задач на статистическом уровне с помощью функции распределения состояния систем ρ исследование должно включать прежде всего спектральное представление операторов: эволюции, микроскопической энтропии, преобразования, внутреннего времени.

5. Важным вопросом является описание непрерывных во времени функций распределения, связанных с незатухающими взаимодействиями, что приводит к появлению сингулярных функций. А это свидетельствует о выходе исследования из гильбертова пространства с «хорошими» функциями и переходе к обобщенным пространствам типа пространства Гельфанда.

Ключевые слова: автоматизированная система; показатели долговечности; асимметрия времени.

РАСЧЕТ СВОЕВРЕМЕННОСТИ ПЕРЕДАЧИ ЗАПРОСА В РЕЖИМЕ ДВОЙНОГО ИСПОЛЬЗОВАНИЯ КАНАЛА СИГНАЛИЗАЦИИ

Косяк Александр Иванович
кандидат технических наук,
МОУ «Институт инженерной физики»,
г. Серпухов, kosyakai@iifmail.ru

Донцов Дмитрий Вячеславович
МОУ «Институт инженерной физики»,
г. Серпухов, info@iifmail.ru

В транкинговых системах радиосвязи в ряде случаев возникает необходимость в периодической передаче детерминированного трафика коротких цифровых сообщений. Примером такой необходимости может служить периодический сбор телеметрии с контролируемых датчиков и приборов учета. В качестве материальной основы для передачи данных сообщений может быть выбран служебный запросный канал связи,

предназначенный для передачи запросов на выделение каналов трафика. Данный подход освобождает от дополнительной нагрузки каналы трафика, предназначенные для передачи информации (голоса и данных) по установившемуся между абонентами соединению. Передача сообщений на фоне запросов возможна посредством организации двойного использования запросного канала связи, состоящего в попеременном использовании канала как для передачи запросов, так и для передачи собираемых сообщений. Сеть радиодоступа характеризуется комплексом показателей. Передача запросов по запросному каналу влияет на своевременность установления соединения, характеризуемую временем установления соединения с вероятностью, не менее заданной. Передача запроса на выделение канала трафика является начальным этапом процедуры установления соединения и своевременность передачи данного запроса напрямую влияет на своевременность выполнения процедуры в целом. К своевременности установления соединения предъявляются жесткие требования, отраженные в соответствующих регламентирующих документах, ввиду чего для организации передачи по служебному запросному каналу связи детерминированного трафика необходимо ответить на следующий вопрос – какой размер пропускной способности можно «взять» у запросного канала в условиях выполнения выдвигаемых требований по своевременности установления соединения и направить его на передачу детерминированного трафика телеметрических сообщений? Целью данной работы является разработка математической модели передачи запроса в режиме двойного использования запросного канала. Данная математическая модель позволяет описать процесс передачи запросов в условиях попеременного использования канала связи и является основой методики расчета вероятностно-временных характеристик доставки запросов на установление соединения. Просчитав для рассматриваемого диапазона значений выделяемой пропускной способности своевременность доставки запроса на основе представленной методики можно будет получить ответ на вопрос о минимально-достаточной пропускной способности, выделяемой для передачи запроса и оценить характеристики процесса сбора телеметрических сообщений.

Ключевые слова: транкинговые системы радиосвязи; передача запроса; неадаптивный тактированный случайный множественный доступ; запросный канал связи; поглощающая конечная марковская цепь.

СЕКЦИЯ № 6

ПРОБЛЕМЫ РАЗВИТИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ В РОБОТИЗИРОВАННОМ КОМПЛЕКСЕ ЗАЧИСТКИ РЕЗЕРВУАРОВ ДЛЯ НЕФТЕПРОДУКТОВ

Багаев Леонид Александрович
ФАУ «25 ГосНИИхиммотологии МО РФ»,
г. Москва, Россия, 25gosniihim@mil.ru

Ерёмин Владимир Николаевич
кандидат технических наук, доцент,
ФАУ «25 ГосНИИхиммотологии МО РФ»,
г. Москва, Россия, 25gosniihim@mil.ru

Инютин Сергей Арнольдович
доктор технических наук, профессор,
ФАУ «25 ГосНИИхиммотологии МО РФ»,
г. Москва, Россия, Inyutin_sa@mail.ru, 25gosniihim@mil.ru

Анализируется разработанная концептуальная модель автоматизации вторичных процессов в экспериментальном образце многофункционального роботизированного комплекса для зачистки внутренней поверхности резервуаров для нефтепродуктов. Подробно описаны структура, состав и процесс функционирования экспериментального образца роботизированного комплекса. Первичный процесс в комплексе удаление с внутренней поверхности резервуара несмываемых остатков нефтепродукта и роботизированную зачистку специальными управляемыми чистящими устройствами, с использованием жидкой фазы моющих средств и специального чистящего раствора, вторичные процессы — мониторинг внутренней поверхности, фильтрация чистящего раствора и удаление из резервуара нефтепродуктов, возникших после зачистки, углеводородного шлама. При функционировании роботизированного комплекса должен выполняться мониторинг внутренней поверхности резервуара с целью обнаружения дефектов по причинам нарушения герметичности в местах массовой сквозной коррозии материала оболочки резервуара, старения и нарушения целостности оболочки и гермеризирующего материала в местах устранения предыдущих дефектов, наложения заплат и других причин. Вероятно возникновение дополнительных дефектов при применении средств механической зачистки внутренней поверхности. Разработаны модели для вероятностной оценки разгерме-

тизации и протечек нефтепродукта из резервуара, введенного в эксплуатацию после зачистки.

Ключевые слова: роботизированный комплекс; зачистка резервуаров для нефтепродуктов; несмываемые остатки нефтепродуктов; углеводородный шлам; моделирование вторичных процессов на роботизированном комплексе; мониторинг внутренней поверхности резервуара.

К ВОПРОСУ О ЗАЩИТЕ НАВИГАЦИОННОГО ОБОРУДОВАНИЯ ОТ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

Котов Валентин Сергеевич

кандидат технических наук,
Военный институт (Военно-морской политехнический) Военного учебно-научного центра Военно-Морского Флота «Военно-морская академия имени Н.Г. Кузнецова»
г. Санкт-Петербург, г. Пушкин, Россия, legkieshagi@ya.ru

Говоров Александр Александрович

Военный институт (Военно-морской политехнический) Военного учебно-научного центра Военно-Морского Флота «Военно-морская академия имени Н.Г. Кузнецова»
г. Санкт-Петербург, г. Пушкин, Россия, legkieshagi@ya.ru

Сидорцов Игорь Александрович

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова,
г. Санкт-Петербург, Россия, legkieshagi@ya.ru

С 2013 года Министерство обороны Российской Федерации приняло на снабжение геоинформационную систему «Оператор». Дальнейшее совершенствование топогеодезического и навигационного обеспечения Вооруженных Сил предполагало создание программно-аппаратного комплекса средств оперативного создания и обновление цифровой информации о местности (ПАК СО ЦИМ). Функционирование данного комплекса должно было включать в себя сбор, учет, хранение и доведение геопространственной информации до органов военного управления и сил (войск). Стержнем создания ПАК СО ЦИМ ВС РФ должны были послужить глобальные спутниковые навигационные систем ГЛОНАСС.

В настоящее время навигационная аппаратура глобальной спутниковой навигационной системы ГЛОНАСС не нашла широкого распространения в системах навигации и наведения вооружения и военной техники из-за низкой помехоустойчивости. Одним из факторов, существенно влияющих на точность навигационной аппаратуры, является воздействие электромагнитных полей.

Для решения задачи увеличения сопротивляемости аппаратуры к воздействиям внешних факторов необходимо рассматривать какие и как из этих факторов будут действовать на устройство в целом, исходя из продолжительности работы прибора, из каких материалов изготовлен и какими мощностями он оперирует в процессе работы. Совершенствованием характеристик прибора позволяет добиться стабильных и высокоточных результатов.

Одним из наиболее эффективных вариантов улучшения стойкости приборов к воздействиям магнитных полей является экранирование. Экранирование - это, в первую очередь, способ защиты от внешнего магнитного поля путем заключения навигационной аппаратуры в экран, благодаря которому электромагнитное поле в экранируемой области оказывается в значительной степени ослабленным. Качество экранирования, то есть степень уменьшения напряженности поля внутри экрана, зависит от качества материала, его размеров и количества экранов. Установлено, что экранирование улучшается, если проницаемость материала выше, и если толщина экрана больше. Однако, слишком большая толщина экрана может привести к чрезмерному повышению погрешности от вихревых токов. Установлено также, что несколько экранов с воздушной прослойкой между ними лучше защищают прибор, нежели один сплошной, имеющей толщину, равной сумме толщин нескольких экранов.

Следует отметить, что экран так же может внести погрешность в показания прибора, обусловленную намагничиванием прибора в поле самого измерительного механизма. Кроме того, качество экранирования улучшается с ростом частоты внешнего переменного поля вследствие увеличения вихревых токов, индуктированных в самом экране. Поэтому, в приборах, рассчитанных для применения при высоких частотах, толщина экрана может быть значительно снижена.

Количественной характеристикой эффективности экранирования является коэффициент экранирования, который показывает во сколько раз напряженность магнитного поля уменьшится за счет экрана.

$$S = H_э / H ,$$

где S — коэффициент экранирования;

$H_э$ — напряженность внутри экрана;

H — напряженность вне экрана.

Примеры видов экранизирующих материалов: металлические, диэлектрические, стёкла с токопроводящим покрытием, специальные металлизированные ткани, токопроводящие краски. Выбор материала экрана производится для достижения требуемой эффективности экранирования в данном диапазоне частот при определённых ограничениях. Эти ограничения имеют связь с массогабаритными характеристиками экрана, его влиянием на экранируемый объект, механической прочностью, устойчивостью экрана против коррозии, технологичностью его конструкции и т.д. Металлические материалы (медь, алюминий, латунь), используемые для экранирования, изготавливаются в виде листов, сеток и фольги. Все эти материалы должны быть устойчивы к коррозионному воздействию при применении соответствующих защитных покрытий.

Для изучения принципа воздействия магнитного поля на точность навигационных приборов было проведено исследование, в которой рассмотрена природа возникновения погрешностей, связанных с внешним и внутренним магнитным полем, а

так же температурой и рассмотрены три метода экранирования приборов. На основе анализа каждого метода сделаны выводы о степени защиты различными материалами измерительных приборов от воздействия внешнего и внутреннего магнитного поля. Все полученные результаты представлены в виде визуальных изображений, графиков и табличных значений.

Ключевые слова: магнитное поле, электромагнитное поле, измерительные приборы, экранирование, навигационная система ГЛОНАСС.

РАЗРАБОТКА ЭКОНОМИЧЕСКИХ МОДЕЛЕЙ РАЗВИТИЯ ТЕХНИЧЕСКИХ СИСТЕМ ПО ЭТАПАМ ЖИЗНЕННОГО ЦИКЛА

Микитенко Игорь Иванович
кандидат технических наук, старший научный сотрудник,
Национальный исследовательский технологический университет
«Московский институт стали и сплавов».
г. Москва, Россия, iimiki@bk.ru

По теории систем и системного анализа любая, в том числе, техническая система в своем развитии проходит, так называемые, этапы жизненного цикла. Характерной особенностью для больших технических систем является их производство, носящее не массовый, а серийный характер. Большие технические системы в своем развитии требуют значительных вложений, особенно на первоначальных этапах в условиях неопределенности – этапах становления и последующей их разработки (проведение научно-исследовательских и опытно-конструкторских работ). Предлагаемые на первоначальных этапах проекты больших технических систем по ряду показателей (в т.ч. и по предстоящим затратам) подвергаются ревизии и окончательному выбору. Выбранные и принятые системы проходят этапы подготовки и серийного производства, сам этап эксплуатации и, по его завершению, – этап снятия с эксплуатации (утилизации), также требующий ассигнований на его выполнение. Из практики развития подобных систем к применению поэтапно могут допускаться сразу несколько видов таких систем. В интересах прогнозирования и одновременного сопровождения планового развития совокупности больших технических систем требуется разработка комплекса взаимосвязанных экономических моделей, позволяющих проводить оценивание затрат как по отдельным системам и по этапам жизненного цикла этих систем, так и всего комплекса систем в целом. При этом следует учитывать, что каждая отдельно взятая большая техническая система, может подключаться к комплексу систем в разное время, иметь свои индивидуальные схемы технологического процесса производства, свои кооперации заводов изготовителей комплектующих и промежуточной сборки узлов, свои временные сроки развития по этапам и особенности на каждом этапе своего жизненного цикла. Основная задача при проведении исследований и формировании обобщенной экономической модели – снижение сте-

пени неопределенности основных экономических факторов и повышение точности расчетов, на основе которых принимаются ответственные управленческие решения в области технической политики развития систем. Значительная разнотипность комплектующего оборудования, техники, узлов, составляющих большие технические системы, множество методов формирования и определения критериев для выработки рациональных решений развития анализируемых систем и ряд других особенностей требуют разработки единой комплексной имитационной системы, учитывающей указанные условия и данные. Одно изделие (образец) системы проходит различные этапы жизненного цикла: от этапа научно-исследовательских и опытно-конструкторских работ до этапа снятия данного изделия с эксплуатации. Каждый этап состоит из интервалов времени, потребляя ресурсы, и каждый образец находиться на своем временном интервале развития системы. Общие затраты на образец и на одну систему в целом складываться из потребных затрат на тактах времени. При этом, при моделировании учитываются коэффициенты снижения затрат на соответствующем этапе жизненного цикла, характеризующие особенности серийного производства (например, уменьшение стоимость образца при производстве от его номера в партии) и другие особенности, понижающие затраты на однотипную группу (серию) образцов. Моделируются различные режимы финансирования развития одной системы или их совокупности, учитываются особенности и могут уточняться получаемые значения для каждого этапа. Особый интерес при моделировании представляет возможность оценки различных вариантов финансирования (деления ассигнований как по долям между системами и в самой системе, так и по времени), а также структурной перестройки взаимосвязи предприятий участвующих в процессе производства и изменения очередности возможных технологических процессов производства образцов. С помощью датчиков случайных чисел, которые настраиваются на определенные типы распределений, при моделировании используются случайные величины и функции, например: функции зависимости полной стоимости процесса опытно-конструкторских работ и этапа подготовки и производства изделий от продолжительности этапов; случайные величины процесса производства образцов — продолжительность изготовления первого образца; показатель, характеризующий уменьшение продолжительности изготовления образца при увеличении числа изделий в партии и другие показатели; случайные величины процесса эксплуатации — продолжительность эксплуатации элементов систем в зависимости от их типа, условий эксплуатации и других факторов; случайные величины процесса снятия образцов с эксплуатации, характерные для рассматриваемого периода. В результате моделирования, исходя из выделенных ассигнований и некоторых других ограничений, на каждом интервале периода развития систем представляется возможным получать как осредненные значения затрат для каждого образца по этапам жизненного цикла отдельной системы, так и общие затраты на систему и всех систем в целом. А также общие суммарные затраты на систему и на комплекс систем для любого временного диапазона. На любом такте времени можно получать ответ о количестве образцов, находящихся на соответствующем этапе жизненного цикла системы (количестве изделий определенного типа), и всего количества изделий по совокупности систем. Целью данной работы является постановка задачи и разработка частных моделей и обобщенной экономической модели развития единого комплекса больших технических систем серийного производства в интересах оценивания текущих и предстоящих затрат, дальнейшего прогнозирования и, на основе предъявляемых данных имитационного моделирования и проводимых расчетов, принятие эффективных управленческих решений по развитию систем. В последующем, на базе сформированной

модели, – построение программного комплекса и создание автоматизированной системы управления процессами разработки, производства, эксплуатации и утилизации больших технических систем с функциями системы поддержки принятия решений. Предлагаемая модель при серийном или штучном производстве изделий будет полезной в конкретных наукоемких направлениях машиностроения и применима, например, в авиационной, космической, судостроительной, горной и др. отраслях промышленности.

Ключевые слова: экономическая модель, большая техническая система; этапы жизненного цикла; оценка затрат на систему; имитационное моделирование развития системы; серийное производство продукции; эффективные управленческие решения.