основным действием, необходимым для предотвращения SQL-инъекций, является полный и жесткий контроль параметров запросов, поступающих в БД, и тщательная проверка БД на этапе ввода в эксплуатацию.

Гречишников Е.В., Стародубцев П.Ю., Стукалов И.В.
Военная академия связи имени С.М.Буденного

МОДЕЛИРОВАНИЕ СИСТЕМЫ ВОЕННОЙ СВЯЗИ, ИНТЕГРИРОВАННОЙ В ЕДИНУЮ СЕТЬ ЭЛЕКТРОСВЯЗИ РОССИИ, ПРИ ВВЕДЕНИИ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Анализ широкомасштабных конфликтов последнего десятилетия убедительно показывает, что стратегия и тактика ведения войн коренным образом изменились. При ведении информационного противоборства нападающая сторона вначале проводит глобальную разведку всей территории противника, затем, не вступая в прямой контакт с его вооруженными силами, уничтожает все его наиболее важные объекты, элементы инфраструктуры, системы управления и связи, используя при этом высокоточное оружие (ВТО), электромагнитное излучение энергии высокого уровня (ЭВУ) и дистанционные программные воздействия (ДПВ).

В этих условиях актуальным становиться вопрос моделирования поведения системы военной связи (СВС) в условиях ведения информационного противоборства. Моделирование широко применяется при планировании операций вооруженных сил (ВС) стран НАТО. Всем современным военным операциям с участием коалиционного блока НАТО предшествовали стадии моделирования военных действий и анализа результатов моделирования. Правильный выбор исходных данных, создание адекватных моделей, грамотный анализ выходных результатов являлись причиной минимизации потерь, скоротечного хода и успешного

исхода проведения операций. При этом моделировались: размещение и комплектация основных и резервных сил и средств, прогнозируемые воздействия каждой из сторон и их последствия, потери сторон и ресурсы сил и средств, система управления (органы и пункты управления), система военной связи как элемент системы управления.

Принимая во внимание тот факт, что система связи является динамически изменяющимся объектом, подверженным различным и трудно прогнозируемым видам воздействий противника, наиболее приемлемыми для создания моделей СВС являются имитационные модели.

В настоящее время в условиях интеграции систем связи различных министерств и ведомств с Единой сетью электросвязи (ЕСЭ) РФ, обеспечивающей предоставление услуг электросвязи пользователям на территории России, а ЕСЭ РФ в свою очередь с международным информационным пространством, наиболее актуальным становиться вопрос моделирования интегрированных систем связи. Сложность моделирования таких систем заключается в правильном формировании исходных данных, описании потенциальных воздействий, как на систему военной связи, так и на ЕСЭ РФ.

Основной целью моделирования является выявление взаимосвязи основных показателей устойчивости элементов СВС с условиями их функционирования при интеграции с ЕСЭ РФ с целью обеспечений операций ВС РФ. Поставленная цель может достигаться путем имитации передачи информационных сообщений между абонентами всех категорий. При этом учитываются вероятные действия иностранных технических разведок (ИТР) и, как следствие их действий, - прогнозируемые воздействия (огневые, электромагнитные излучения и дистанционные программные) противника. Также необходимо учитывать возможности системы восстановления элементов СВС.

Задача создания модели СВС, как объекта воздействия противника в условиях использования ресурсов ЕСЭ РФ, должна включать в себя ряд основных этапов:

выбор и обоснование основных показателей устойчивости (как одного из основных свойств системы связи) элементов СВС в условиях применения ИТР и внешних деструктивных воздействий: огневого поражения; электромагнитной энергии высокого уровня, дистанционных программных воздействий.

содержательное описание модели СВС, интегрированной с ЕСЭ РФ, как объекта воздействия противника;

описание СВС и ЕСЭ РФ в виде систем и сетей массового обслуживания (СМО и СеМО);

разработка имитационной модели СВС, интегрированной с ЕСЭ РФ, как объекта воздействия противника и её оценка.

Выбор и обоснование показателей устойчивости элементов СВС и математического аппарата для моделирования СВС, как объекта воздействия противника, осуществляется, руководствуясь требованиями руководящих документов и опыта войск.

Модель СВС, как объекта воздействия противника выполняется с учетом особенностей использования СВС в условиях общевойсковых операций при ведении информационного противоборства.

Содержательное описание модели включает в себя основные этапы, такие как:

задание структуры обобщённой модели СВС, как объекта воздействия противника;

учет характеристик фрагмента ЕСЭ РФ с арендованными в интересах СВС каналами и цифровыми потоками;

разработка моделирующих алгоритмов (имитации огневых, электромагнитной энергии высокого уровня, а также программных воздействий).

При учете характеристик обобщённой модели СВС, как объекта воздействия противника учитываются основные факторы, влияющие на устойчивость элементов СВС.

При разработке фрагмента ЕСЭ РФ учитываются структура, топология и состав сети, многообразие предоставляемых телекоммуникационных услуг. Интеграция ЕСЭ РФ в мировое информационное пространство, обеспечивает доступность основных элементов ЕСЭ иностранным разведкам. Соответственно, ЕСЭ РФ как в мирное, так и в военное время наиболее уязвима для компьютерной разведки и дистанционных программных воздействий.

Основу имитационной модели составляет алгоритм моделирования. В ходе разработки моделирующего алгоритма имитации воздействий огневых, электромагнитной энергии высокого уровня, дистанционных программных на основе анализа статистики, выбираются основные типы воздействий и ранжируются по степени нанесения ущерба элементам СВС, т.е. по степени влияния как на устойчивость СВС, так и на своевременность обслуживания абонентов различных категорий. При этом должна быть учтена интеграция СВС с ЕСЭ РФ. Учитывая тактико-технические характеристики современных мобильных, многофункциональных узлов связи военного назначения, привязка к ЕСЭ РФ может осуществляться одновременно через несколько узлов доступа, по различным интерфейсам и протоколам передачи данных. В свою очередь это позволит оперативно моделировать изменение структуры и топологии СВС, за счет реконфигурации и перемещения элементов СВС.

При моделировании в качестве основных видов разведок, действующих против элементов СВС необходимо учитывать

радиолокационную, инфракрасную, радиоразведку и техническую компьютерную разведку. В качестве прогнозируемых внешних деструктивных воздействий на СВС в модели целесообразно учитывать огневое поражение и воздействия электромагнитной энергией высокого уровня и особенно дистанционные программные воздействия. В качестве наиболее актуального на сегодняшний день воздействия, как в угрожаемый период, так и военное время.

При разработке моделирующего алгоритма имитации внешних деструктивных воздействий должны учитываться ошибки ИТР. Ошибками 1-го рода считаются ошибки в определении местоположения, функциональной принадлежности и других элементов СВС силами и средствами ИТР. Ошибками 2-го рода считаются ошибки при обнаружении несуществующих (ложных) объектов, не соответствующих реальным элементам СВС.

Разработка имитационной модели СВС интегрированной с ЕСЭ РФ, как объекта воздействия противника, может включать в себя следующие этапы:

выбор и обоснование математического аппарата для построения модели;

представление СВС интегрированной с ЕСЭ РФ в виде систем и сетей массового обслуживания (СМО и СеМО);

разработку моделирующего алгоритма СВС как объекта воздействий противника с учетом функционирования СВС совместно с ЕСЭ РФ;

программную реализацию модели;

оценку качества разработанной модели.

В ходе выбора и обоснования математического аппарата, используемого для построения модели, проводится анализ разработанного моделирующего алгоритма с позиций возможности представления его различными видами моделирования. Затем производится выбор языка

моделирования. После чего СВС и ЕСЭ РФ как сети массового обслуживания представляются в виде графов с описанием структуры с помощью матриц связности и маршрутизации.

Алгоритм моделирования функционирования СВС интегрированной с ЕСЭ РФ, как объекта воздействия противника, формализовано представляет содержательное описание функционирования СВС интегрированной с ЕСЭ РФ. При этом должны учитываться выбранные маршруты прохождения арендованных основных и резервных каналов связи, цифровых потоков, алгоритмы имитации ИТР и деструктивных воздействий противника с учетом особенностей современных военных операций и содержания информационного противоборства, а также имитация подсистемы восстановления.

Программная реализация математической модели должна осуществляться с учетом следующих требований:

программа должна быть выполнима при заданных ресурсах ПЭВМ по производительности и оперативной памяти;

структура программы должна обеспечивать возможность модернизации, дополнения и расширения функций модели, программа должна быть простой и удобной в эксплуатации;

программа должна позволять проводить однозначную оценку правильности функционирования программы при заданных исходных данных;

при помощи программы должно быть обеспечено повторение заданных условий проведение любого эксперимента в диапазоне условий, выбранных для испытаний.

Оценка качества разработанной модели проводится по таким направлениям как: оценка адекватности, точности и достоверности, а также проведение предварительных исследований на модели.

Основными исходными данными для разработки модели могут являться:

состав и топология элементов СВС;

структура фрагмента ЕСЭ РФ с арендованными в интересах СВС цифровыми потоками, основными и резервными каналами связи;

основные характеристики арендованных цифровых потоков, каналов связи;

количество арендованных цифровых потоков, основных и резервных каналов по направлениям связи;

среднее время восстановления связи;

время переключения потоков различного уровня и иерархии скоростей;

вероятность потерь элементов СВС в результате воздействия ВТО (функционального поражения, дистанционного программного);

возможности подсистемы восстановления (требуемое значение укомплектованности элементов СВС, время доставки средств связи на все уровни восстановления, вероятности выхода из строя элементов СВС из-за внешних воздействий, время развёртывания резервных элементов СВС, количество резервных элементов СВС, производственные возможности ремонтных органов и др.)

В качестве ограничений и допущений предполагаются:

структура, состав и топология ЕСЭ РФ известны противнику и доступны для воздействий;

структура ЕСЭ РФ имеет заданный ресурс для резервирования арендованных в интересах СВС каналов и трактов;

применительно к этапу моделирования мирного времени и угрожаемого периода рассматривается как стационарный, так и полевой компонент СВС;

применительно к этапу моделирования военного времени рассматривается только полевой компонент СВС;

рассматриваются воздействия: ВТО (ЭВУ), дистанционные программные воздействия.

Основными выходными результатами модели являются: основные показатели устойчивости элементов СВС: коэффициенты готовности, оперативной готовности и исправного действия, вероятность выживания элемента СВС, вероятность своевременного восстановления связи.

В качестве выходных зависимостей могут быть: зависимость основных показателей своевременности обслуживания абонентов от вероятности поражения элементов СВС определенными видами воздействий, зависимости вероятности выживания элементов СВС от разведзащищенности для различных видов ИТР, зависимости вероятности своевременной передачи сообщений, от вероятности выживания элемента для различных видов воздействий, зависимость своевременности обслуживания абонентов от разведзащищенности, живучести или устойчивости СВС.

Программная реализация модели может быть осуществлена в таких средах программирования как GPSS, SIMPAS, DELPHI и других.

Таким образом, разработанная концептуальная модель позволит разработать строго формализованную математическую модель СВС как объекта воздействия противника, в которой будут учитываться изменившиеся условия ведения военных действий, а также особенности функционирования СВС при использовании ресурсов ЕСЭ РФ. По результатам моделирования возможно выявление функциональных зависимости основных свойств СВС друг от друга, что позволит осуществлять рациональный выбор данных для развертывания СВС, в условиях использования ресурсов ЕСЭ РФ.

Разработанная модель может использоваться в учебном процессе высших военных учебных заведениях, при исследовании вопросов организации связи в ходе проведения современных операций, а также различными должностными лицами органов военного управления на этапах планирования, организации и функционирования военной связи.

Стародубцев Ю.И., Семенов С.В.

Военная академия связи имени С.М.Буденного

АНАЛИЗ ИМЕЮЩИХСЯ ПОДХОДОВ К РАЗРАБОТКЕ И ОПТИМИЗАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Способность Вооруженных Сил выполнять поставленные задачи в значительной мере определяются эффективностью функционирования системы связи, которая в значительной мере зависит от степени автоматизации процессов управления связью. Теоретические принципы построения и оптимизации таких систем ориентированы на улучшение основных показателей функционирования (в основном быстродействие).

Однако интеграция систем автоматизации (как управления, так и связи) накладывает особые требования по обеспечению безопасности информации и функционирования системы, а так же систем автоматизацию которых она осуществляет. На современном этапе развития теории построения (разработки) автоматизированных систем связи вопросам безопасности уделяется не достаточное внимание. К тому же эти вопросы ставятся в конце цикла разработки, а зачастую уже во время функционирования системы. Безопасность приходится обеспечивать за счет внесения дополнительных подсистем и модулей, которые должны учитывать структуру, возможности и другие характеристики уже сформированной системы и пытаться каким-либо образом подстроиться под нее. Такой подход приводит к малоэффективной и кратковременной