

развитии математических и логических средств моделирования, а также предложены различные формальные и графические нотации, отражающие специфику решаемых задач.

ПОСТРОЕНИЕ ЗАЩИЩЁННЫХ СЕТЕВЫХ ПРИЛОЖЕНИЙ НА БАЗЕ CRYPTOAPI

О.В. Кошкин, П.Е. Негинский

Научный руководитель – к.т.н., доцент *Н.А. Разорёнов*
Белорусский национальный технический университет

Основная цель данной работы – это показать возможности и преимущества использования CryptoAPI при построении сетевых приложений с архитектурой клиент-сервер.

Задачи, которые ставит настоящий доклад: изучить состояние проблемы на современном этапе развития сетевых приложений; показать архитектуру CryptoAPI; показать возможности применения CryptoAPI при построении сетевого приложения; предложить свой пример построения защищённого сетевого приложения.

С массовым внедрением компьютеров во все сферы деятельности человека объем информации, хранимой в электронном виде, вырос в тысячи раз. И теперь скопировать за полминуты и унести дискету с файлом, содержащим план выпуска продукции, намного проще, чем копировать или переписывать кипу бумаг. А с появлением компьютерных сетей даже отсутствие физического доступа к компьютеру перестало быть гарантией сохранности информации.

Рост объема информации, передаваемой через сеть Интернет, переводит сведения, содержащиеся в ценных сообщениях, документах и финансовых расчетах, в разряд потенциально незащищенных данных. Это рождает необходимость в эффективном механизме защиты. Говоря о сетевой безопасности, следует затронуть две непростые темы: шифрование и аутентификация. Если мы хотим скрыть нашу информацию от злоумышленника, то нам требуется перемещать и маскировать её, используя специальные двунаправленные технологии, позволяющие проводить шифрование и дешифрование с высоким уровнем надежности при разумных затратах. Если мы хотим обмениваться сообщениями, то механизм аутентификации должен гарантировать надежную идентификацию общающихся сторон.

Технологии, которые позволяют привнести целостность, надежность и защищенность в программный код и данные, можно объединить под одним названием – криптография. Набор существующих в операционной системе Windows функций, воплощающих теоретическую модель в конкретную реализацию, носит название CryptoAPI. Существует также версия CryptoAPI SDK, использующая COM интерфейсы.

В данной работе будет продемонстрировано использование криптографии в реальном приложении. В начале будет объяснена архитектура и программная модель CryptoAPI. Далее, большее внимание будет уделено самим функциям. Конечной целью является создание защищённого сетевого приложения на базе CryptoAPI и описание механизма безопасного обмена ключами на базе алгоритма RSA. В качестве алгоритма шифрования основных данных выбран поточный алгоритм RC4.

КОНСТРУИРОВАНИЕ СИЛОВЫХ СИСТЕМ С РЕЖИМОМ ОПТИМАЛЬНОГО БЫСТРОДЕЙСТВИЯ

Д.А. Дука

Научный руководитель – к.т.н., доцент *А.Н. Мацкевич*
Военная академия Республики Беларусь

Важнейшими показателями боевой эффективности комплексов вооружения (самоходных артиллерийских установок (САУ), зенитных самоходных установок (ЗСУ), танков, БМП и др.) являются: возможность применения оружия при защитном маневре, быстрая реакция на поставленную задачу, минимальное время обнаружения и захват цели, высокие показатели

точности и кучности стрельбы. Эти показатели в большой степени зависят от характеристик приводов наведения и стабилизации (ПНС) вооружения, средств разведки, обнаружения и сопровождения цели, таких, как точность и плавность слежения, диапазон регулируемых скоростей, значения максимально регулируемых скоростей и ускорений. Поэтому для большинства современных комплексов вооружения стоит одна из важнейших задач – создание быстродействующих приводов наведения и стабилизации с широким диапазоном регулирования скорости при высокой точности слежения с наличием ограничений на плавность перемещения нагрузки, особенно в области низких скоростей.

Основными этапами проектирования силовых систем являются: выбор и обоснование функциональной схемы; выбор и расчет параметров исполнительного устройства; выбор и расчет параметров усилительно-преобразовательных элементов; выбор и расчет параметров измерительного элемента; разработка математической модели силовой системы; расчет требуемого коэффициента преобразования; выбор корректирующих элементов и расчет параметров управляющего устройства силовой системы.

Исходя из требований к точности обработки задающего воздействия, а также качества работы системы в переходном и установившемся режимах выбирается желаемое управляющее устройство. Для силовой следящей системы в качестве желаемой передаточной функции выбирается ПИД-регулятор. Этот выбор справедлив, поскольку обеспечиваются допустимая скоростная ошибка системы, заданный запас устойчивости по фазе, а также локальные показатели качества переходного режима.

В целях повышения быстродействия приводов необходим синтез оптимального по быстродействию управляющего устройства. Это можно обеспечить за счет непосредственного синтеза устройства оптимального по быстродействию, синтеза оптимальных систем по быстродействию с использованием принципа максимума и синтеза оптимальных систем по быстродействию методами классического вариационного исчисления.

Анализ результатов математического моделирования силовых систем с режимом оптимального быстродействия, проведенных с использованием выше указанных подходов, показывает, что быстродействие приводов с оптимальным управляющим устройством в 2-3 раза меньше, чем в штатной силовой системе.

АВТОНОМНЫЙ МОБИЛЬНЫЙ РОБОТ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А.А. Кустиков

Научный руководитель – к.т.н., доцент *П.П. Шардыко*
Белорусский национальный технический университет

В последнее время в различных странах мира достигнут большой прогресс в разработке мобильных роботов (МР) различного назначения. Также разрабатывается большое число связанных с этой областью информационных технологий, связанных с различными аспектами функционирования таких систем. К этим направлениям можно отнести различные алгоритмы распознавания образов, обработки изображений, алгоритмы синтеза модели окружающего мира на основе данных от датчиковых систем робота, алгоритмы планирования траекторий с учетом недетерминированной внешней среды и многое другое.

При оснащении МР различными бортовыми спецсредствами, они трансформируются в мобильные робототехнические комплексы (МРТК). В задачи МРТК специального назначения может входить ликвидация последствий чрезвычайных ситуаций, спасательные операции, предотвращение террористических актов, ведение радиационной, химической и боевой разведки и пр. Многие из этих задач актуальны для РБ. Научный и производственный потенциал республики позволяет создавать МРТК такого класса самостоятельно.

Целью данной работы являлась разработка концепции МР, который служил бы базой для различных модификаций МРТК специального назначения. Для достижения этой цели решались был проведен статистический анализ характеристик МР различных образцов и применяемых в них технических решений. На основании статистических данных и с учетом условий и имеющихся наработок в РБ разработана следующая конструктивная компоновка шасси