

качество разработки электронных схем.

На сегодняшний день существует множество программных продуктов прикладного назначения, вобравших опыт и знания многих специалистов в области электроники и электротехники. На практике для моделирования и отладки электронных схем значительное распространение получил программный пакет ELECTRONICS WORKBENCH, благодаря дружественному пользовательскому интерфейсу, наглядно-графической форме проектирования, а также адекватности математической модели реальным электронным элементам. Данный пакет был использован при постановке лабораторных работ в курсах, связанных с изучением принципов работы и проектированием электронных схем аналоговых и цифровых устройств систем автоматизации и средств робототехники. Это позволяет значительно расширить количество возможных вариантов исследуемых схем, глубже и нагляднее изучать влияние различных элементов схем на работу устройств в целом. Данный подход вносит творческое начало в учебный процесс.

Практически без значительных материальных затрат (что немаловажно в условиях ВУЗа) можно обновлять объекты изучения и расширять возможности студентов в самостоятельной работе. Такой подход в сочетании с работой на реальных лабораторных стендах позволяет повысить качество подготовки специалистов.

## ОДИН ИЗ ПОДХОДОВ К ОФОРМЛЕНИЮ ДОКУМЕНТАЦИИ ПО СТУДЕНЧЕСКИМ ПРОГРАММНЫМ РАЗРАБОТКАМ

*Е.Д. Белькевич*

Научный руководитель – к.т.н., доцент *О.В. Бугай*  
*Белорусский национальный технический университет*

При объектно-ориентированном подходе к разработке программного обеспечения в основном находит применение спиральная модель его жизненного цикла. При этом процесс разработки программного изделия представляют в виде схемы, показанной на рис. 1.

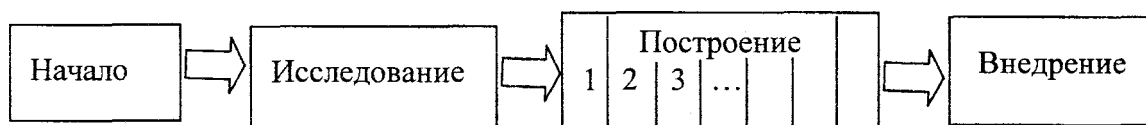


Рис. 1. Процесс разработки программного изделия

Это итеративный и нарастающий процесс, при котором программное обеспечение разрабатывается и реализуется по частям. Фаза построения состоит из многих итераций, на каждой из которых выполняются построение, тестирование в настоящее время практика и интеграция высококачественного программного продукта, удовлетворяющего некоторому подмножеству требований к проекту. Каждая итерация содержит все обычные фазы жизненного цикла программного обеспечения: анализ, проектирование, реализация и тестирование. При переходе от итерации к итерации диаграммы, иллюстрирующие предмет разработки уточняются и на последней стадии разработки представляют собой модель завершённой программы.

Существующая в настоящее время практика оформления документации к студенческим программным изделиям, как правило, фиксирует окончательный результат, а поэтому плохо иллюстрирует ход процесса разработки. Целью данного доклада является введение в особенности современных методов и средств оформления и логического или информационного моделирования программного обеспечения.

Процесс разработки адекватных моделей и их последующего конструктивного применения требует не только знания общей методологии системного анализа, но и наличия соответствующих изобразительных средств или языков для фиксации результатов моделирования и их документирования. Очевидно, что естественный язык не вполне подходит для этой цели, поскольку обладает неоднозначностью и неопределённостью. Для построения моделей были разработаны достаточно серьёзные теоретические методы, основанные на

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