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 приемущесва 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 назащищенных 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 перемешивать 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 Widows 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