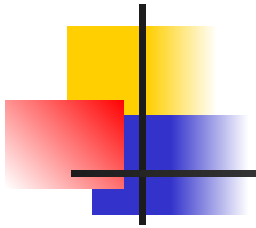
Криптография и компьютерная безопасность

Борисов В.А.
КАСК – филиал ФГБОУ ВПО РАНХ и ГС
Красноармейск 2011 г.

- Особую актуальность вопросы использования криптографических средств и методов защиты информации приобрели в связи с распространением общедоступных сетей передачи данных и повсеместного их применения в хозяйственной деятельности человека.



- Активное развитие криптографического инструментария оказывает стимулирующее влияние на становление специфических областей человеческих знаний.

Проблемы, связанные с обеспечением ИБ

- импортные компоненты не могут считаться доверенными;
- использование разнородных и часто мало совместимых программно-аппаратных составляющих;
- повсеместное использование открытых сетей передачи данных.

Направления построения информационных систем

- использование стандартизованных и общепринятых идеологий, методов и средств в случае, если цели и требования, закладываемые в реализацию проекта, могут быть достигнуты путем унифицированных решений;
- применение частных решений, обеспечивающих специфические потребности.

- Средства защиты информации могут быть также унифицированными в зависимости от идеологии и архитектуры построения информационно-телекоммуникационной системы, создаваемой для решения конкретных задач.

Проблемы, связанные с обеспечением ИБ

- защита информационных ресурсов локальной рабочей станции от несанкционированного доступа;
- защита в локальных сетях передачи данных;
- защита межсетевого взаимодействия;
- создание защищенных виртуальных сетей на базе общедоступных сетей передачи данных;
- обеспечение защиты технологии клиент/сервер;

Проблемы, связанные с обеспечением ИБ

- защита информационных ресурсов корпоративной сети, имеющей выход в общедоступные сети передачи данных, от атак извне;
- средства защиты пользовательского взаимодействия;
- защита электронной почты и документооборота;
- защита электронных платежных систем.

Требования к выбору ключевых систем

- устойчивость ключевой системы к компрометации ключей;
- у пользователей должно находиться минимальное число ключей;
- предусматривать защиту от копирования;
- иметь механизмы плановой смены ключей и сертификатов открытых ключей.

Требования к эффективности применения систем защиты информации

- масштабируемость;
- интегрируемость;
- контролируемость;
- структурированность;
- сертифицируемость;
- эшелонированность.

Требования к быстродействию средств защиты

- эффективная обработка мультиплексированных данных на уровне пакетов;
- средства безопасности не должны вносить существенные задержки в процесс обработки и передачи информации;
- эффективные средства обновления ключей;
- обработка больших объемов информации в единицу времени;
- работа в системах с различной пропускной способностью.

Интеграция аппаратных средств

- Заключается в разработке и реализации физических процедур сопряжения подобных средств защиты информации в целевую систему.

- Программные средства защиты информации могут быть реализованы:

  -в виде законченного программного продукта,

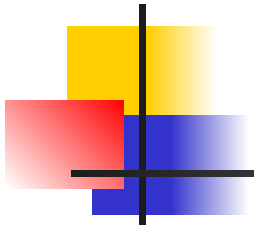
  -в виде дополнительных процедур модулей, встраивающихся в программное обеспечение целевой системы.

Способы встраивания программных средств защиты информации

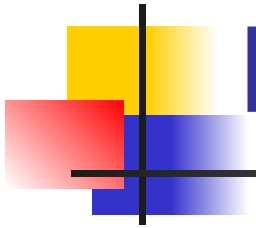
Способы встраивания программных средств защиты информации

с использованием программных интерфейсов

с использованием криптосервера

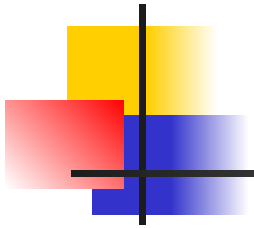


- Основная проблема встраивания заключается в корректном использовании вызываемых функций.



Программный интерфейс

- Детальное описание функций и используемых ими параметров.



- Для того, чтобы интегрировать защитный механизм в данное ПО, необходимо согласовать форматы функций.

- Средства защиты информации подразделяются в зависимости от уровня взаимодействия открытых систем.

Вероятные угрозы физического и канального уровней

- несанкционированное подключение,
- ошибочная коммутация,
- прослушивание,
- перехват,
- фальсификация информации,
- имитоатаки,
- физическое уничтожение канала связи.

- Для защиты информации на данном уровне обычно применяют скремблирование, шифрующие модемы, специализированные канальные адаптеры.

Достоинства реализации средств защиты физического и канального уровней

- простота применения;
- аппаратная реализация;
- полная защита трафика;
- прозрачность выполнения средствами защиты информации своих функций.

Недостатки применения средств защиты канального и физического уровней

- негибкость решения;
- низкая совместимость,
- высокая стоимость.

Задачи сетевого уровня

- защита информации непосредственно в пакетах, передаваемых по сети;
- защита трафика сети;
- контроль доступа к ресурсам сети.

Угрозы для сетевого уровня

- анализ служебной информации сетевого уровня;
- атаки на систему маршрутизации;
- фальсификация IP-адресов;
- атаки на систему управления;
- прослушивание, перехват и фальсификация информации;
- имитоатаки.

Способы устранения угроз сетевого уровня

- пакетная фильтрация;
- административная защита на маршрутизаторах;
- протоколы защиты информации сетевого уровня;
- туннелирование;
- векторизация;
- динамическое распределение сетевых адресов;
- защита топологии.

Достоинства средств защиты сетевого уровня

- полнота контроля трафика;
- универсальность;
- прозрачность;
- совместимость;
- адаптивность к сетевой топологии.

Недостатки средств защиты сетевого уровня

- неполнота контролируемых событий.

Опасные угрозы транспортного уровня

- несанкционированные соединения, разведка приложений;
- атаки на систему управления;
- прослушивание, перехват и фальсификацию информации;
- имитоатаки.

Решения проблем транспортного уровня

- защита в составе межсетевых экранов;
- proxy-системы;
- протоколы защиты транспортного уровня.

Достоинства средств защиты транспортного уровня

- развитая функциональность;
- высокая гибкость защиты.

Недостатки средств защиты транспортного уровня

- неполнота защиты;
- неподконтрольность событий в рамках прикладных и сетевых протоколов.

Прикладной уровень

- Зашифрованная информация разбивается на пакеты и сетевые кадры, надежность доставки которых обеспечивается транспортной средой.

Основные угрозы прикладного уровня

- НСД к данным;
- разведка имен и паролей пользователей;
- атаки на систему разграничения прав доступа пользователей;
- маскировка под легитимного пользователя;
- атаки на систему управления, атаки через стандартные прикладные протоколы;
- фальсификация информации;
- имитоатаки.

Защита информации ресурсов прикладного уровня

- встроенная защита приложений,
- межсетевые экраны с фильтрацией прикладных протоколов,
- proxy-системы и т.д.

Достоинства размещения средств защиты прикладного уровня

- полнота и высокая функциональность в рамках конкретного приложения;
- контроль на уровне действий конкретного пользователя.

Недостатки средств защиты прикладного уровня

- отсутствие универсальности,
- ограниченность рамками заданного набора приложений,
- неподконтрольность событий в нижележащих уровнях управления.