Защита программных средств защищенных телекоммуникационных систем

Разрушающие программные средства

Угрозы безопасности информации и программного обеспечения КС возникают как в процессе их эксплуатации, так и при создании этих систем, что особенно характерно для процесса разработки ПО, баз данных и других информационных компонентов КС.

Безопасность программного обеспечения в широком смысле является свойством данного программного обеспечения функционировать без проявления различных негативных последствий для конкретной компьютерной системы.

В настоящее время одним из наиболее опасных средств информационного воздействия на компьютерные системы являются программы - вирусы или компьютерные вирусы.

Под *компьютерным вирусом следует понимать программы*, способные размножаться, прикрепляться к другим программам, передаваться по телекоммуникационным каналам

Алгоритмическая закладка – это умышленно спрятанная часть кода программы, из-за действия которой изменяются программные функции в ряде случаев, данные функции не предусмотрены программным описанием и нигде не заявлены. Запуск скрытых функций происходит при выполнении определённых условий в ходе вычислительных процессов компьютерной системы

Программная закладка – это внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций, позволяющих осуществлять несанкционированные воздействия на информацию

Модели действий программных закладок:

1. Перехват данных:

a) перехват вывода информации на экран;

b) перехват ввода с клавиатуры;

c) перехват и обработка файловых операций;

d) копирование и пересылка конфиденциальной пользовательской информации.

2. Искажение данных:

a) неадекватная реакция на команды пользователя;

b) искажение передаваемой по сети информации;

c) блокирование принимаемой или передаваемой по сети информации;

d) изменение функционала самой программы.

3. Уничтожение данных:

a) уничтожение конфиденциальной пользовательской информации;

b) инициирование программных и аппаратных сбоев.

4. получение несанкционированного доступа к данным:

a) получение управления некоторой функцией в обход системы авторизации;

b) получение доступа к данным и функциям с непредусмотренных периферийных устройств..

Обобщенная классификация *разрушающих программных средств*

- компьютерные вирусы - программы, способные размножаться, прикрепляться к другим программам, передаваться по линиям связи и сетям передачи данных, проникать в электронные телефонные станции и системы управления и выводить их из строя;

- программные закладки - программные компоненты, заранее внедряемые в компьютерные системы, которые по сигналу или в установленное время приводятся в действие, уничтожая или искажая информацию, или дезорганизуя работу программно-технических средств;

- способы и средства, позволяющие внедрять компьютерные вирусы и программные закладки в компьютерные системы и управлять ими на расстоянии.

Основные типы РПС

- *РПС, отключающие защитные функции системы.*
- *Перехватчики паролей.*
- *Программные закладки, превышающие полномочия пользователя.*
- *Логические бомбы.*
- *Мониторы.*
- *Сборщики информации об атакуемой среде.*

Модели взаимодействия прикладной программы и программной закладки

- *Модель «перехват».*
- *Модель «троянский конь».*
- *Модель «наблюдатель».*
- *Модель «компрометация».*
- *Модель «искажение или инициатор ошибок».*
- 6. *Модель «сборка мусора».*

Методы внедрения РПС

- *Маскировка закладки под «безобидное» программное обеспечение.*
- *Маскировка закладки под «безобидный» модуль расширения программной среды.*
- *Подмена закладкой одного или нескольких программных модулей атакуемой среды.*
- *Прямое ассоциирование.*
- *Косвенное ассоциирование.*

ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПО

- *Принципы обеспечения технологической безопасности при обосновании, планировании работ и проектном анализе ПО*
- *Принципы достижения технологической безопасности ПО в процессе его разработки*

- *Принципы обеспечения технологической безопасности на этапах стендовых и приемо-сдаточных испытаний*
- *Принципы обеспечения безопасности при эксплуатации программного обеспечения*