УДК 004.05

Основы анализа инцидентов для обнаружения вредоносного программного обеспечения

Автор: Идришев.А.М
Satbayev University , Казахстан г.Алматы
Научный руководитель: лектор, Зиро А.А.
Satbayev University , Казахстан г.Алматы

Аннотация

В данной статье рассмотрены аспекты информационной безопасности в отношении вредоносного программного обеспечения и их анализ.

Введение

В наши дни анализ способствует получению важной информации об инцидентах. Специалист должен уметь идентифицировать доказательства, при этом анализировать и , в случае обнаружения , устранять вредоносное программное обеспечение.

Основная часть

Любая программа , предназначенная для нарушения работы ПО , сети и конфиденциальности информации , является вредоносной. Анализ вредоносной программы предназначен для исследования ее работы и дальнейшего устранения.

Для обеспечения безопасности ПО, сети и конфиденциальности информации существуют множество вариантов противодействия вредоносному программному обеспечению.

Анализ вредоносного программного обеспечения является сложной задачей для специалиста по информационной безопасности. Кроме этого , у каждого специалиста есть свой основной метод или анализ выявления вредоносного ПО. В основном используются следующие виды анализов:

- Базовый статический анализ;
- Поведенческий анализ;
- Сетевой анализ;
- Расширенный динамический анализ;
- Расширенный статический анализ;
- Автоматический анализ.

В данной статье будут исследованы различные виды анализа инцидентов и разработана методика по устранению вредоносного программного обеспечения.