

Расширенная стохастическая модель распространения вредоносного кода.

Сидоров Михаил Владимирович
e-mail: johnnythesame@gmail.com

Ершов Игорь Валерьевич

Задача противодействия распространению вредоносных кодов является актуальной проблемой на сегодняшний день. Компании, работа которых, так или иначе, связана с использованием передачи данных по сетям, терпят убытки от постоянных вспышек эпидемий сетевых червей, новые модификации которых появляются практически день. К сожалению, современное программное обеспечение не способствует снижению числа новых эпидемий вредоносных программ, которые находят все новые уязвимости в различных программах. Противодействовать распространению вредоносных программ достаточно сложная задача, которая имеет множество аспектов, одним из которых является моделирование распространения вредоносных программных продуктов. Эта работа является продолжением исследований в области изучения существующих моделей распространения. Были рассмотрены особенности стохастических, детерминистских, физических и других видов моделей, выявлены их преимущества и недостатки.

В качестве наилучшей была выбрана стохастическая модель, как наиболее соответствующая к реальным условиям. На ее основе была разработана новая модель прогнозирования. Ее преимуществами являются учет метода распространения и топологии сети. В рамках работы были проведены теоретические исследования для глобальных сетей, обладающих значительным числом взаимных физических связей между узлами.