УДК 004.942

ОБ ОСОБЕННОСТЯХ МОДЕЛИРОВАНИЯ ПРОЦЕССА РАСПРОСТРАНЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ГЛОБАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

© Царева А.А., Задорина Н.А.

e-mail: tzaryova.alina1998@gmail.com

Рыбинский государственный авиационный технический университет имени П.А. Соловьёва, г. Рыбинск, Российская Федерация

В настоящее время вредоносное программное обеспечение (ПО) наносит большой ущерб организациям и отдельным пользователям компьютеров. Благодаря масштабам глобальных сетей и высоким пропускным способностям современных каналов связи, вредоносные программы могут быстро инфицировать большое число рабочих станций. Отсюда следует необходимость прогнозирования распространения вредоносного ПО в глобальных сетях.

Существует несколько основных различий между глобальными и локальными сетями, которые определяют различия в прогнозировании процесса распространения вредоносного ПО в этих сетях.

Таблица 1. Сравнение глобальных и локальных сетей

Показатели	Глобальные сети	Локальные сети
Количество рабочих станций	Не ограничено	Ограничено
Скорость передачи	Низкая	Высокая
Качество каналов связи	Низкое	Высокое
Поддержка различных топологий	Есть	Есть

Исходя из основных различий между глобальными и локальными сетями, можно выделить особенности распространения вредоносного ПО в компьютерных сетях:

1. Неограниченное число рабочих станций, подверженных заражению.
2. Отсутствие возможности учета характеристик отдельных компьютеров.
3. Возможность потери пакетов вследствие некачественной связи.
4. Низкая скорость распространения вредоносного ПО, по сравнению с распространением в локальных сетях, вследствие низкой скорости передачи данных.

Для прогнозирования процесса распространения вредоносного ПО в сетях используется аналитическое, имитационное и натурное моделирование. Каждый из подходов имеет свои особенности.

Основной проблемой при прогнозировании является то, что количество компьютеров в глобальной сети может меняться и то, что учесть характеристики отдельных компьютеров невозможно.

Так как глобальная сеть рассчитана на неограниченное количество узлов, натурное моделирование в этих условиях невозможно.

Имитационное моделирование заменяет исходную систему моделью, достаточно точно описывающей ее в значимых для данного исследования характеристиках. Так как одной из основных особенностей в прогнозировании распространения вредоносного ПО в глобальных сетях является неограниченное число рабочих станций, прогнозирование с помощью имитационного моделирования достаточно сложная задача. Это обуславливается большим количеством машин в сети, которые должны

быть учтены в модели, а также тем, что в глобальных сетях зачастую происходит подключение и отключение рабочих станций в произвольный момент времени (количество станций в сети – переменная величина).

Аналитическое моделирование представляет собой замену исходной системы некоторыми функциональными соотношениями, которые отражают только общие характеристики системы.

Аналитическая модель SI, например, предполагает наличие двух типов объектов: зараженные (I) и незараженные (S). Данная модель может применяться для прогнозирования распространения вредоносного ПО в компьютерных сетях. Однако, она не учитывает возможность перехода из состояния «зараженный» в состояние «незараженный», поэтому относительно точный прогноз может быть только на ранних стадиях развития эпидемии.

Модель SIR учитывает наличие вылеченных объектов. Поэтому данная модель является более точной, чем примитивная модель SI.

Модель PSIDR является двухэтапной моделью. На первом этапе заражение происходит, как в модели SI. На втором этапе начинается «поиск» зараженных компьютеров и их «вакцинация».

Модель SAIR учитывает наличие компьютеров с антивирусным ПО, поэтому использование данной модели для прогнозирования процесса распространения вредоносного ПО в глобальных сетях невозможно, ввиду отсутствия возможности учета особенностей отдельных узлов сети.

Таким образом, можно сделать следующие выводы о применимости различных подходов для прогнозирования процесса распространения вредоносного ПО в глобальных сетях:

1. Натурное моделирование не применимо.
2. Имитационное моделирование применимо для прогнозирования, однако в связи с большим количеством рабочих станций данное прогнозирование будет занимать достаточно большое количество времени. Также имитационное моделирование имеет преимущество перед аналитическим моделированием, только когда учитывается достаточно большое количество параметров сети, а в прогнозировании распространения вредоносного ПО в глобальных сетях невозможно учесть характеристики отдельных компьютеров.
3. Аналитическое моделирование применимо, поскольку не требует больших вычислительных затрат, и в большей части моделей не учитываются те параметры, определение которых в глобальных сетях затруднено или невозможно.

3.1. Модель SI применима, однако она будет давать приближенный прогноз.

3.2. Модель SIR применима для прогнозирования, так как учитывает возможность излечения объектов.

3.3. Модель PSIDR применима для прогнозирования и является наиболее точной, так как учитывает то, что процесс излечения начинается только через какое-то время после заражения.

3.4. Модель SAIR не применима для прогнозирования, так как предполагает учет параметров конкретных компьютеров (наличие антивирусного ПО).

Библиографический список

1. Новиков С.В. Модель распространения вирусных атак в сетях передачи данных общего пользования на основе расчета длины гамильтонова пути [Текст]: автореф. дис. на соиск. учен. степ. канд. техн. наук (19.02.2008) / Носков Сергей Валерьевич; СПб ГУ ИТМО. – Санкт-Петербург, 2007.– 94 с.

2. Кельтон В., Лоу А. Имитационное моделирование. Классика CS. 3-е изд. – СПб.: Питер; Киев: Издательская группа BHV, 2004. – 847 с.: ил.