ИЕРАРХИЧЕСКАЯ МОДЕЛЬ ТЕСТИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРИ НЕЧЕТКОМ ОПИСАНИИ СПЕЦИФИКАЦИИ

Н.А. ВОЛОРОВА, В.И. НОВИКОВ, А.А. ПОПОВА

Для сложных систем при условии нечеткого описания спецификации даже в одной выделенной области количество тестовых сценариев, как правило, достаточно велико и для их наилучшей организации необходимо прибегать к вероятностному анализу.

Допустим, что тестовые сценарии можно представить в виде n параллельных ветвей. Обращение к системе может продвигаться по одной из ветвей. В таком представлении вероятность нахождения ошибки выполнения ветви может быть вычислена с учетом вероятности выбора i-й ветви и вероятности успешного прохождения ветви.

Вероятность выбора той или иной ветви кейса тестирования программного продукта может быть установлена на основе экспертной оценки.

Используя данный метод можно определить, на какие варианты использования из множества тестовых сценариев необходимо выделить больше ресурсов и в соответствии с этим разработать адекватную для конкретных условий модель тестирования. Удачно выбранная модель тестирования позволяет дать максимально полную и актуальную информацию о наиболее вероятных рисках связанные с выпуском системы.

АНАЛИТИЧЕСКИЕ МОДЕЛИ DDOS АТАК

В.И. НОВИКОВ, Л.В. НОВИКОВА

Объектами защиты в системах и сетях передачи данных являются:

– данные IP пакетов, передаваемые по защищенному каналу в рамках частной виртуальной сети;

– инфраструктура передачи данных (аппаратные и программные средства, встроенное программное обеспечение, каналы связи, интерфейсы подключения к сети передачи данных);

– атрибуты безопасности узлов сети (криптографические ключи, таблицы маршрутизации, списки доступа и информация конфигурации);

– аутентификационные данные пользователей;

– аппаратные и программные средства управления безопасностью;

– сообщения инцидентов безопасности, данные аудита безопасности и статистика по работе сети;

– информация управления сетью.

В работе проведен анализ проблемных задач защиты информации, среди которых выделены недостаточно исследованные проблемы моделирования атак на ИС. Проведен обзор видов атак, выполнена их классификация. Для моделирования одних из наиболее распространенных DoS и DDoS атак разработаны стохастические дискретные и непрерывные модели, позволяющие оценить степень воздействия атак этих типов на ИС в функции от степени защищенности ИС. Обсуждаются результаты аналитического и численного расчета моделей.

КОГНИТИВНОЕ КОДИРОВАНИЕ ИНФОРМАЦИИ В МНОГОПОЛЬЗОВАТЕЛЬСКОЙ СЕТИ

С.Б. САЛОМАТИН, А.А. ОХРИМЕНКО, И.В. САДЧЕНКО

Одно из основных требований по обеспечению безопасности в сетях передачи данных состоит в том, что обмен критичными данными (транзакциями) должен выполняться только посредством надежного канала или носителя, которые гарантируют аутентичность содержания, доказательства отправления и получения, а также невозможность отказа от факта обмена данными.