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.

Рассматривается многопользовательский канал с подслушиванием (МКП). Используется два кодера с когнитивной связью, в том смысле, что одному кодеру априори известно некоторое сообщение другого кодера.

Предполагается, что в МКП передаются с разными скоростями два независимых сообщения.

Кодирование сообщений осуществляется двумя пользователями с использованием независимых случайных переменных с произвольной энтропией. Один из пользователей работает в режиме когнитивного кодирования и кодирует два сообщения. Второй пользователь кодирует только одно из двух сообщений.

Декодеры легитимного и подслушивающего приемников работают в разных условиях приема.

Когнитивная модель передачи информации создает для подслушивающего узла сети режим приема на фоне помехи, что снижает эффективность подслушивания и обеспечивает в топологии сети области с надежной связью.

Метод позволяет создать защищенный регион сети, в котором скорости передачи, удовлетворяют требуемым неравенствам.

КОДОВАЯ ЗАЩИТА В СЕТЕВЫХ СТРУКТУРАХ С ОШИБКАМИ И ПЕРЕХВАТОМ ИНФОРМАЦИИ

Т.А. АНДРИЯНОВА, С.Б. САЛОМАТИН

В сетевых структурах, использующих элементы с разным уровнем защиты, возможен перехват информации скрытыми агентами, а также возникновение разного рода ошибок в процессе передачи информации по каналам связи. Информация в таких сетевых объектах может быть защищена путем внесение кодовой избыточности и разнесение путей передачи информации.

Одними из механизмов сетевого кодирования являются коды, которые представляются в виде упорядоченных пар подпространств расширенного конечного поля.

Модель направленной сети связи имеет вид графа $G=(V, E)$, где V — множество узлов сети, а E — множество ребер — коммуникационных линий. Предполагается, что порядок E ассоциирован с частичным порядком G. Возможно мультиплексирование ребер между парами узлов. Через каждое ребро графа может быть передан один символ поля. Для сети G линейный код сетевого кодирования определяется как множество локально кодированных ядер вейвлет-функций.

Источник информации имеет M узлов сети, обеспеченных кодовыми фильтрами избыточного кода A. Доверенные узлы используют фильтрами избыточного кода B.

За один сеанс связи узел-получатель получает множество пакетов, прошедшие через узлы сети с кодированием фильтровой системой. Процесс декодирования основан на возможности восстановления информации с помощью вейвлет-преобразования в конечных полях.

Эффективность кодирования оценивается по скорости, с которой информация может быть надежно и безопасно доставлена требуемым узлам сети.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЛАТЕЖЕЙ В СИСТЕМАХ ЭЛЕКТРОННОЙ КОММЕРЦИИ

О.Б. ЗЕЛЬМАНСКИЙ, С.М.М. ГОНДАГ, Ш.М.Г. МОЗДУРАНИ

Современные информационные системы активно внедряются в банковской сфере, что позволяет банкам предоставить клиентам широкий спектр услуг, в том числе обеспечить возможность проведения удаленных транзакций. Несомненные удобства таких взаимодействий, с одной стороны, порождают проблему аутентификации и авторизации