

Модель инсайдера на основе сетей Петри-Маркова

Дубинич Е. А. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Белов Н. И. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Научный руководитель – к.т.н., доцент Кузнецов А. Ю. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Введение. В данной работе был рассмотрено информационное взаимодействие «Инсайдер – система защиты» с потенциальными и различными возможностями сторон. Сеть Петри-Маркова, представленная в данной работе, изображает процесс конфликта. Представленные интегрально-дифференциальные уравнения описывают информационные конфликты, а также обосновывают выбор паттернов с целью исследования его динамических характеристик. Представлен алгоритм работы программно-аппаратного комплекса для возможности создания модели процесса указанного конфликта. Так же как многие отраслевые стандарты, бизнес-процессы, модель и нотация, событийно-управляемые цепочки процессов, UML диаграммы. Сети Петри предполагают графические обозначения для процессов, отображаемые поэтапно и включающие в себя возможность выбора, итерации и одновременное выполнение. Основным отличием от всех остальных стандартов, сеть Петри имеет четкие математические определения для использования с семантикой и отлично развитой математической теорией анализа процесса.

Основная часть. В большинстве организаций имеется ряд сотрудников, обладающих фактически неограниченным доступом к информационным системам. Сотрудники IT-отдела, обычно имеют базу логинов и паролей, знают как организована система, имеют доступ к электронным подписям сотрудников компании, имеют возможность очищать различные данные, даже информацию об утечках.

Заключение. В ходе проделанной работы была предложена модель умышленного воздействия инсайдера на информационную систему с целью получения, построенная с использованием математического аппарата сетей Петри-Маркова. Приведена система интегро-дифференциальных уравнений для описания сети, которую, обладая необходимой информацией о законе распределения времени перемещения из состояния в переход, возможно применить при расчете времени прохождения этапов и вероятности реализации воздействия. Для дальнейшего исследования необходимо определить подходящий закон распределения, а также возможно усложнение модели, путем появления дополнительных переходов и состояний, которые более точно учитывают реальное поведение инсайдера.

Дубинич Е. А. (автор)

Белов Н. И. (соавтор)

Кузнецов А. Ю. (научный руководитель)