П. А. Арьков (Волгоград, ВолГУ)**. Построение модели процесса реализации угрозы в информационной системе на основе сети Петри.**

Современные информационные системы (ИС) участвуют в автоматизации документооборота предприятий и учреждений, поддерживают различные бизнес-процессы, управляют производством и т. д. Организация систем защиты информации (СЗИ) подобных ИС регламентируется различными нормативными документами. Однако в документах процесс оценки СЗИ носит характер требований присутствия в системе тех или иных средств защиты, при этом игнорируются вопросы вероятности преодоления данных средств за счет уязвимостей, присутствующих в них.

В работе, представленной данным сообщением, предлагается модель, которая позволяет оценить вероятность реализации угрозы и время, затрачиваемое на реализацию угрозы. Рассматривается ординарная временная сеть Петри $N = (P_l, T, F, W, M_0)$. Здесь P_l — множество мест сети $P_1 = S \cup \{V_1\} \cup Th \cup F_1$, где S — злоумышленник, $\{V_l\}$ — уязвимости СЗИ, Th — реализация угрозы, F_l — провал попытки реализации угрозы. Множество переходов T представляет собой фактически множество способов эксплуатации той или иной уязвимости. Для времен переходов используется логнормальный закон распределения плотности вероятностей. Начальная разметка сети M_0 такова: $M_0(P_{l_i}) = 0$ при $P_{l_i} \in S$, $M_0(S) = 1$.

Для разрешения конфликтов используется предварительный выбор по вероятности срабатывания перехода, которая интерпретируется как вероятность выбора злоумышленником данного способа эксплуатации уязвимости.

Анализ данной сети осуществляется моделированием. Моделирование проводится до достижения либо места Th, либо F_l, либо до достижения сетью состояния, в котором не сможет сработать ни один переход.

В рамках данной модели были рассчитаны вероятности реализации для таких угроз факультетской локальной вычислительной сети, исходящих от студентов университета, как: уничтожение открытых файлов на файл-сервере, раскрытие конфиденциальных файлов преподавателейб хранимых на файл-сервере, отказ в обслуживании домена сети и т. д.