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

В любом административном органе субъекта федерации функционирует информационная система (ИС), обрабатывающая большие объемы данных различного уровня конфиденциальности. Вопросы защиты информации в подобных системах регулируются руководящими документами Федеральной службы по техническому и экспортному контролю, которые рассматривают требования к используемым средствам и методам защиты, не рассматривая при этом варианты их преодоления или обхода.

В работе, представленной данным сообщением, предлагается модель преодоления системы защиты, предназначенная для расчета вероятности и среднего времени осуществления угрозы для ИС.

Модель представляет собой полумарковский процесс с конечным множеством состояний $\{V\} = \{V_l\} \cup T \cup F$, где $\{V_l\}$ — множество уязвимостей СЗИ, T — угроза ИС, F — провал попытки реализации угрозы. При этом, исходя из специфики моделируемого процесса, все состояния являются невозвратными, а состояния T и F — поглощающими. Переходы из состояния i в состояние j представляют собой способ эксплуатации i-й уязвимости системы защиты.

В рамках рассматриваемой модели время пребывания в состоянии интерпретируется как время, необходимое злоумышленнику на эксплуатацию i-й уязвимости при условии, что в дальнейшем он перейдет в j-е состояние (уязвимость, к реализации угрозы или атака провалится). Функция $F_{ij}(x)$, отображающая время пребывания в состоянии, описывается логнормальным распределением.

Кроме того, задается начальное распределение $p_i^{(0)} = \mathbf{P}\{v_1 = i\}$, определяющее, из какого состояния злоумышленник начнет преодоление СЗИ, и матрица вероятностей выбора следующего перехода ($p_{ij}^{\text{перех.}}$), которая определяет вероятность выбора пути преодоления СЗИ злоумышленником. Учитывая, что при том или ином способе эксплуатации уязвимости есть вероятность неудачи и провала атаки в целом, для каждого перехода рассматриваемого процесса задаются вероятности $P_{ij}^{\text{усп.}}$ успешной эксплуатации i-й уязвимости и вероятность $P_{ij}^{\text{пров.}}$ провала атаки при попытке эксплуатации i-й уязвимости. При этом $P_{ij}^{\text{усп.}} + P_{ij}^{\text{пров.}} = 1$. Тогда элементы матрицы переходных вероятностей (p_{ij}) полумарковского процесса, где $j \in \{V_l\} \cup T \cup F$, представляют собой следующее:

$$p_{ik} = p_{ik}^{\text{перех.}} P_{ik}^{\text{усп.}} \quad \text{при} \quad k \in \{V_l\} \cup T, \quad p_{iF} = \sum_j p_{ij}^{\text{перех.}} P_{ij}^{\text{пров.}}.$$

Поиск решения проводится моделированием этого полумарковского процесса.

С применением данной модели получены следующие результаты для угрозы нарушения конфиденциальности информации сотрудников на файл-сервере факультетской сети.