**Д. В. Кириллов** (Самара, СамГУ)**. Управление распространением полномочий на основе рисков в событийно-обусловленном делегировании и отзыве полномочий.**

Модель событийно-обусловленного делегирования и отзыва полномочий (СОДОП) [1] позволяет автоматизировать процесс выполнения операций по делегированию и отзыву полномочий в системах, реализующих контроль доступа на основе ролей (КДОР) и контекстно-ориентированную модель КДОР в качестве механизмов разграничения доступа.

При формировании графа распространения прав доступа большую роль играют ограничения, накладываемые на отношения назначения пользователей на роли, назначения полномочий ролям и отношения допустимости делегирования полномочий. Ограничения могут иметь вид как четко формально заданных критериев, связанных с характеристиками элементов и отношений системы, так и нечетко заданных критериальных границ, основанных на некоторых статистических и вероятностных характеристик поведения и свойств системы. Первый вариант ограничений достаточно подробно исследован в работах, связанных с проблемой распределения обязанностей и конфликта интересов в контроле доступа на основе ролей [2], второй вариант, реализуемый на основе метода анализа рисков, исследован относительно полно только в работах, связанных непосредственно с механизмами КДОР [3] и контекстно-ориентированного КДОР. В моделях делегирования полномочий данный метод задания ограничений ранее не был рассмотрен.

Особенность подхода, предложенного автором, заключается в том, что кроме риска, связанного с выполнением операций, вводится также зависимость рисков от атрибутов объектов, субъектов и ролей, участвующих в выполнении операции. В качестве ограничений на выполнение операций делегирования и отзыва полномочий выступают веса дуг, связывающих элементы множеств пользователей, постоянных ролей, делегированных ролей, объектов и их атрибутов. При этом веса дуг динамически корректируются в зависимости от компетенции пользователей, выполняющих как системные операции, так и операции делегирования полномочий, причем в расчете учитываются все ребра цепочки делегирования. В качестве показателей рисков могут выступать как числовые значения, так и качественные показатели решетки ценности информации. Предложенный подход позволяет достигнуть высокого уровня детализации при формировании и реализации политики безопасности в контексте автоматизированной информационной системы.

СПИСОК ЛИТЕРАТУРЫ


1. *Кириллов Д. В.* Основные принципы событийно-обусловленного делегирования и отзыва полномочий. — Вестник УГАТУ, 2009, т. 1 (30).
2. *Nyanchama M.*, *Osborn S.* The role graph model and conflict of interest. — ACM Transactions on Information and Systems Security, 1999, v. 2, № 1, p. 3–33.
3. *Nissanke N.*, *Khayat E. J.* Risk based security analysis of permissions in rbac. — In: Proceedings of the 2nd international workshop on information systems, 2004.