МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАТИКА, МАТЕМАТИКА, АВТОМАТИКА

ІМА :: 2013

МАТЕРІАЛИ
та програма

НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

(Суми, 22-27 квітня 2013 року)

Суми
Сумський державний університет
2013

Защита данных системы управления документами от несанкционированного доступа

Стержанов М.В., *доц.*
Белорусский государственный университет информатики и радиоэлектроники, г. Минск

Одним из важнейших принципов разработки системы управления документами (СУД) Stagirites является обеспечение защиты информации от несанкционированного доступа. Права на элементы контента выдаются абстрактной сущности “Опекун”, в качестве которой может выступать пользователь системы, группа, системная учетная запись. Избирательное управление доступом реализовано с использованием списка контроля доступа (СКД) [1]. Каждая запись СКД содержит идентификатора узла дерева контента, идентификатор «Опекуна», маску прав, тип, маску наследования.

Помимо доступа к элементам контента реализована разграничение доступа пользователей к различным вспомогательным модулям, входящим в состав СУД (например «Загрузка данных», «Преобразование данных», «Управление пользователями»). Все пользователи системы в ходе своей работы явно или неявно обращаются к различным данным. В качестве таких данных могут выступать элементы контента, конфигурации системы, а также файлы, используемые в процессе работы системы. Данные логически объединяются и хранятся в контейнере, называемом группой данных (ГД). Помимо обращения к данным, пользователь выполняет над данными различные операции. В качестве таких операций можно выделить: изменение содержания, удаление, создание новых объектов данных. Набор логически связанных операций называется группой операций (ГО). Для получения одновременного доступа к ГД и ГО введено понятие роли. Роль является совокупностью некоторых возможностей пользователя в системе. Обладание ролью дает право доступа ко всем объектам данных и операций, входящих в ГД и ГО, относящихся к этой роли. При назначении роли определяется период действия, т.е. доступ к некоторому модулю системы устанавливается на определенный период времени (возможно, неограниченный).

1. Pfleeger, S.L. Pfleeger, *Security in Computing* (New Jersey: Prentice Hall: 2003).