О. В. Л у к и н о в а (Москва, ИПУ РАН)**. Структуризация механизмов защиты и отображение их на модель OSE|RM.**

В докладе рассматривается отображение механизмов защиты (Mx) как межкатегорийных сервисов (Cross-Category Services) на структуру модели среды открытых систем OSE|RM [1], включающей несколько плоскостей (базовую, администрирования, защиты и др.). Это дает возможность иметь референсную функциональность не только базовой плоскости, но и плоскости защиты. Структуризация осуществлялась в несколько этапов.

Вначале все множество механизмов было поделено на 3 группы.

Группа 1. Целевые — обеспечивающие основные свойства безопасности (критерии, обеспечиваемые системой безопасности) $\{\overline{KS}\} = \{C, D, K\}$, где C — целостность, D — доступность, K — конфиденциальность данных, которые должны быть свойственны реализациям любой «клетки» всех трех плоскостей модели, т. е. каждая «клетка» должна быть «закрыта» с точки зрения K, C, D.

Группа 2. Обеспечивающие, т. е. те Mx, которые осуществляют дополнительные действия, необходимые для организации функционирования целевых Mx и осуществления Mx своей цели на том или ином уровне безопасности.

Группа 3. Механизмы управления — обеспечивают контроль и согласованное функционирование Mx 1-й и 2-й групп.

Именно Mx-управления реализуются в виде приложения плоскости администрирования, составляющего суть системы управления безопасностью информационной системы.

Каждый Mx — референсный и представляет собой иерархию механизмов-подклассов, действия которых направлены на разные объекты OSE|RM. Для дальнейшей структуризации необходимо было представить внутреннюю структуру Mx. Для этого были использованы модели в виде онтологий. На рис. 1 представлен класс защитных механизмов, на основе которого разработаны экземпляры конкретных Mx.

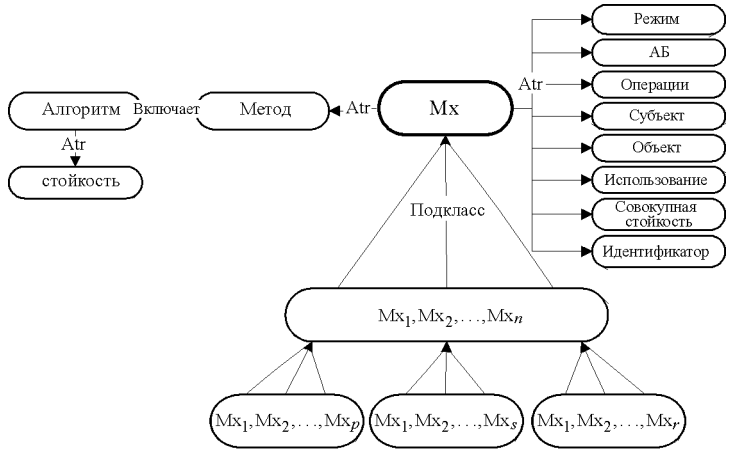

Рис. 1. Онтология класса Mx

Третий этап структуризации заключался в том, что механизмы-подклассы (листья таксономий) необходимо было сопоставить «клеткам» всех трех плоскостей модели OSE|RM. В качестве примера такого сопоставления можно рассмотреть реализацию операций над данными, декларируемых [2]: хранение; обработка; передача за пределы действия политик безопасности (ПБ); передача внутри и между влиянием ПБ. Эти операции могут быть легко отражены на соответствующих плоскостях модели (см. пример операции на рис. 2).

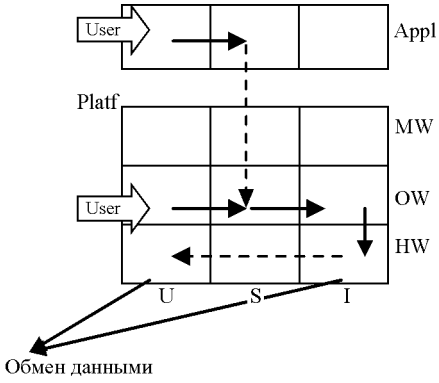

Рис. 2. Передача данных на съемные носители, инициируемая пользователем с использованием средств ОС или формы приложения

Таким образом, операция, «разложенная» по «клеткам», определяет набор Mx, требуемых для защиты операции.

Реализация данного подхода обеспечивает решение трех задач. Во-первых, структуризация Mx позволит реализовать в системе безопасности такие свойства открытости, как расширяемость и масштабируемость, во-вторых, комплексно описывать компоненты плоскости защиты соответствующими стандартами и спецификациями и, в-третьих, представление операций на плоскости с привязкой к ним Mx позволяет говорить об автоматизации процесса проектирования системы безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. ISO/IEC TR 14252-96 Information technology. Guide to the POSIX Open System Environment (OSE).
2. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности.