Математическое и компьютерное моделирование:
материалы III Международной научной конференции
(Омск, 12 ноября 2015 г.). Омск, 2015. С. 189–190. УДК 65.012.810

С.В. Усов

Омский государственный университет им. Ф.М. Достоевского, г. Омск

ПРИМЕНЕНИЕ ОБЪЕКТНО-ОРИЕНТИРОВАННЫХ МОДЕЛЕЙ ПОДСИСТЕМ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ ДЛЯ ПРЕДСТАВЛЕНИЯ СУБЪЕКТНО-ОБЪЕКТНЫХ ПОЛИТИК БЕЗОПАСНОСТИ

Наряду с традиционным субъектно-объектным подходом к моделированию подсистем безопасности компьютерных систем, в настоящее время начинает применяться и объектно-ориентированный подход, при котором каждый элемент компьютерной системы одновременно обладает свойствами как объекта, так и субъекта. Дискреционные политики безопасности в рамках парадигмы объектно-ориентированных систем были построены в работе [1]. В частности, был предложен объектно-ориентированный аналог модели Харрисона–Руззо–Ульмана, OOHRU. Отдельное внимание было уделено системам с иерархией, в которых, в частности, выполнялось правило «нет чтения вверх» применительно к каждому праву доступа, что приближает иерархическую OOHRU к мандатным политикам безопасности [2].

Представляет большой интерес вопрос о том, насколько класс систем, представимых моделью OOHRU шире классов систем, представимых классическими субъектно-объектными моделями безопасности, такими как модели HRU, Take-Grant, Bella–LaPadula [2] и другими. Возможна ли реализация перечисленных политик безопасности средствами OOHRU вообще? Для ответа на этот вопрос был доказан ряд утверждений, который приводится ниже.

1. Объектно-ориентированная модель HRU реализует субъектно-объектную модель HRU.

2. Существует объектно-ориентированная модель Σ, для которой не найдется субъектно-объектной модели, которую бы реализовывала Σ.

3. Объектно-ориентированная модель HRU реализует субъектно-объектную модель HRU с типизированной матрицей доступов (TAM).

4. Объектно-ориентированная модель HRU реализует субъектно-объектную модель Take-Grant.

5. Для любой безопасной ds-свободной модели Белла–ЛаПадулы существует реализующая ее иерархическая модель OOHRU.

6. Для любой безопасной модели Белла–ЛаПадулы существует реализующая ее модель OOHRU.

7. Для любой «классической» мандатной политики безопасности существует реализующая ее иерархическая модель OOHRU.

Первые пять утверждений были доказаны еще в работе [1]. Прокомментируем два последних утверждения. Модель Белла–ЛаПадулы, или МБЛ [3], не является чисто мандатной, поскольку кроме традиционных для мандатных политик ограничений «нет чтения вверх» и «нет записи вниз» в МБЛ присутствует и элемент дискреционной политики в виде матрицы доступов. Под ds-свободной МБЛ подразумевается модель, в которой матрица доступов не накладывает никаких дополнительных ограничений на доступ субъекта к объекту. Таким образом, с помощью модели OOHRU достаточно реализовать ограничение «нет записи вниз», а это можно сделать с помощью создания двух копий для каждого объекта в иерархической OOHRU, причем первая копия будет подчинена иерархии по чтению, а вторая – иерархии по записи. Кроме того, результаты утверждения 5 справедливы и для классических мандатных моделей, поскольку в них матрица доступов отсутствует изначально.

Термин «безопасная МБЛ» трактуется с точки зрения так называемой Basic Security Theorem [3]. Важно отметить, что в при доказательстве утверждений 5 и 6 строится дискреционная модель, безопасная с точки зрения МБЛ, однако возможность проверки ее безопасности с точки зрения дискреционных политик безопасности не установлена.

Литература

1. *Усов С.В.* Неоднородные объектно-ориентированные модели с иерархией // Проблемы обработки и защиты информации. Кн. 3. Модели разграничения доступа: монография / Под общ. ред. С.В. Белима. Омск: КАН, 2013. С. 93–114.

2. *Гайдамакин Н.А.* Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во Уральского Университета, 2003.

3. *Bell D.E., LaPadula L.J.* Secure Computer System: Unified Exposition and Multics Interpretation. Technical report 2997, rev. 1. MITRE, 1996.