Защита данных пользователя

Смирнов Д.

К высокоуровневым целям безопасности относятся защита данных пользователя и защита функций безопасности объекта оценки. Соответствующие классы функциональных требований характеризуются большим числом входящих в них семейств и разнородностью компонентов.

Класс FDP (защита данных пользователя) включает тринадцать семейств, которые можно разбить на четыре группы:

- политики защиты данных пользователя;
- виды защиты данных пользователя;
- импорт и экспорт данных пользователя;
- защита данных пользователя при передаче между доверенными изделиями ИТ.

Политики защиты данных пользователя

В первую группу входят два семейства - FDP_ACC (политика управления доступом) и FDP_IFC (политика управления информационными потоками), - играющие, по сути, формальную роль именования политик, распространяющихся на определенные множества субъектов, объектов (потоков) и операций. Управление может быть ограниченным и полным. В последнем случае требуется, чтобы все операции всех субъектов на любом объекте (потоке) из области действия функций безопасности были охвачены некоторой политикой.

Виды защиты данных пользователя

Вторая группа объединяет семь семейств. Содержательные аспекты управления доступом (информационными потоками) регламентируются семействами FDP_ACF (функции управления доступом) и FDP_IFF (функции управления информационными потоками). Первое устроено очень просто, состоит из одного компонента и требует наличия политик, основанных на атрибутах безопасности, а также дополнительных правил, явно разрешающих или запрещающих доступ.

Требования к функциям управления информационными потоками, представленные шестью *компонентами*, существенно сложнее и многообразнее.

Семейство FDP_DAU (аутентификация данных) обслуживает один из видов статической целостности данных.

Семейство FDP_ITT (передача в пределах ОО) содержит требования, связанные с защитой данных пользователя при их передаче по внутренним каналам объекта оценки. Предусматривается базовая защита внутренней передачи (FDP_ITT.1), направленная на предотвращение раскрытия, модификация ситуаций недоступности, а также мониторинг целостности данных (FDP_ITT.3).

Согласно требованиям семейства FDP_RIP (защита остаточной информации), унаследованным от "Оранжевой книги", функции безопасности должны обеспечить уничтожение любого предыдущего содержания ресурсов при их выдаче и/или освобождении.

Семейство FDP_ROL (откат) предусматривает возможность отмены последней операции и возврат к предшествующему состоянию с сохранением целостности данных пользователя.

Последнее семейство второй группы, FDP_SDI (целостность хранимых данных), содержит требования мониторинга целостности всех контролируемых объектов и выполнения заданных действий при обнаружении ошибок целостности хранимых данных

Импорт и экспорт данных пользователя

В третью группу семейств класса FDP, обслуживающую импорт и экспорт данных пользователя в/за пределы области действия функций безопасности объекта оценки, мы включили, как и следовало ожидать, два сходных по структуре двухкомпонентных семейства: FDP_ETC (экспорт) и FDP_ITC (импорт). Они различаются по наличию или отсутствию (использованию или игнорированию) ассоциированных с данными атрибутов безопасности. Согласованная интерпретация атрибутов оговорена экспортером и импортером.

Защита данных пользователя при передаче между доверенными изделиями ИТ.

В последнюю, четвертую группу (защита данных пользователя при передаче между доверенными изделиями ИТ) входят два семейства, ведающих обеспечением конфиденциальности (FDP_UCT) и целостности (FDP_UIT). Имеется в виду, что одним из доверенных изделий является объект оценки, а для передачи используются внешние (по отношению к ОО) каналы.

FDP_UCT состоит из одного компонента, требующего защиты от несанкционированного раскрытия.

В семейство FDP_UIT включены более содержательные требования. Во-первых, предусматривается всеобъемлющая защита от модификации, удаления, вставки и повторения данных. Во-вторых, обнаруженная ошибка целостности может быть восстановлена как с помощью отправителя, доверенного изделия ИТ, так и силами самого объекта оценки.

Обратим внимание на различие требований к защите данных пользователя при передаче по внутреннему (семейство FDP_ITT) и внешнему (семейства FDP_UCT и FDP_UIT) каналам, что можно считать проявлением гибкости "Общих критериев". Для внешних каналов требования заданы более детально (особенно это касается целостности), однако не предусматривается обеспечение высокой доступности данных.

Отметим также, что за различные аспекты целостности данных пользователя отвечают пять семейств: FDP_DAU, FDP_ITT (точнее, компонент FDP_ITT.3), FDP_ROL, FDP_SDI и FDP_UIT. Первое контролирует аутентичность избранных наборов данных, компонент FDP_ITT.3 и семейство FDP_UIT отвечают за (динамическую) целостность передаваемых данных, FDP_ROL - за восстановление целостности после сбоев или ошибок, а FDP_SDI предусматривает тотальный мониторинг статической целостности.

Спасибо за внимание.