Общая модель ГОСТ Р ИСО/МЭК 15408-1-2012, доработка требований безопасности для конкретного применения

Семиноженко Д. В. ИБО-ФМ-19

Область применения

Настоящий стандарт устанавливает основные понятия и принципы оценки безопасности ИТ, а также определяет общую модель оценки, которой посвящены различные части стандарта, предназначенного в целом для использования в качестве основы при оценке характеристик безопасности продуктов ИТ

В данном стандарте определяются различные операции, посредством которых функциональные компоненты и компоненты доверия, приведенные в ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3, могут быть доработаны для конкретного применения путем использования разрешенных операций

Объект оценки

Примерами ОО являются:

- прикладная программа;
- операционная система;
- прикладная программа в сочетании с операционной системой;
- прикладная программа в сочетании с операционной системой и рабочей станцией;
- операционная система в сочетании с рабочей станцией;
- интегральная схема смарт-карты;
- локальная вычислительная сеть, включая все терминалы, серверы, сетевое оборудование и программные средства;
- приложение базы данных за исключением программных средств удаленного клиента, обычно ассоциируемых с приложением базы данных

Операции

При использовании операций разработчик ПЗ/ЗБ должен также отследить, чтобы зависимости других требований, которые зависят от данного требования, были удовлетворены. Разрешенные операции выбирают из следующей совокупности:

ПЗ — Профиль защиты

ЗБ—Задание по безопасности

итерация (iteration): позволяет неоднократно использовать компонент при различном выполнении в нем операций;

назначение (assignment): позволяет определять параметры;

выбор (selection): позволяет выбирать один или более пунктов из перечня;

уточнение (refinement): позволяет осуществлять детализацию.

Операции "назначение" и "выбор" разрешены только в тех местах компонента, где они специально обозначены. Операции "назначение" и "выбор" разрешены для всех компонентов. Операции выбора при необходимости можно сочетать с итерацией. В этом случае применение выбранного варианта для каждой итерации не должно пересекаться с предметом другой итерации выбора, так как они должны быть уникальными.

Операции

Операция "итерация"

Операция "итерация" может быть выполнена по отношению к любому компоненту. Разработчик ПЗ/ЗБ выполняет операцию "итерация" путем включения в ПЗ/ЗБ нескольких требований, основанных на одном и том же компоненте. Каждая итерация компонента должна отличаться от всех других итераций этого компонента, что реализуется завершением по-другому операций "назначение" и "выбор" или применением по-другому операции "уточнение". Различные итерации следует уникально идентифицировать, чтобы обеспечить четкое обоснование и прослеживаемость от или к этим требованиям. Различные итерации следует уникально идентифицировать, чтобы обеспечить четкое обоснование и прослеживаемость от или к этим требованиям. В ряде случаев операция "итерация" может быть выполнена по отношению к компоненту, для которого вместо его итерации можно было бы выполнить операцию "назначение", указав диапазон или список значений. В этом случае разработчик ПЗ/ЗБ может выбрать наиболее подходящую альтернативу, решив с учетом всех обстоятельств, есть ли потребность предоставления единого обоснования для всего диапазона значений или необходимо иметь отдельное обоснование для каждого из значений. Разработчику также следует обратить внимание на то, требуется ли отдельное прослеживание для этих значений.

Операция "назначение"

Операцию "назначение" осуществляют тогда, когда рассматриваемый компонент включает элемент с некоторым параметром, значение которого может быть установлено разработчиком ПЗ/ЗБ. Параметром может быть ничем не ограниченная переменная или правило, которое ограничивает переменную конкретным диапазоном значений.

Операция "назначение"

Каждый раз, когда элемент в ПЗ предусматривает операцию "назначение", разработчик ПЗ должен выполнить одно из четырех действий:

1. Оставить операцию "назначение" полностью невыполненной. При достижении или превышении определенного числа неуспешных попыток аутентификации должны выполнить [назначение: спис действий]
2. Полностью выполнить операцию "назначение". При достижении или превышении определенного числа неуспешных попыток аутентификации должны предотвращать в дальнейшем привязку соответствующей внешней сущности к какому-либо субъекту;
3. Ограничить операцию "назначение", чтобы в дальнейшем ограничить диапазон допустимых значений.
4. Преобразовать "назначение" в "выбор", ограничивая таким образом "назначение". При достижении или превышении определенного числа неуспешных попыток аутентификации должны осуществить [выбор: предотвращать в дальнейшем привязку соответствующего пользователя к какому-либо субъекту, уведомлять администратора].

Операция "выбор

Операцию "выбор" осуществляют тогда, когда рассматриваемый компонент включает элемент, в котором разработчиком ПЗ/ЗБ должен быть сделан выбор из нескольких пунктов. Каждый раз, когда элемент в ПЗ предусматривает операцию "выбор", разработчик ПЗ может выполнить одно из трех действий:

1. оставить операцию "выбор" полностью невыполненной;
2. полностью выполнить операцию "выбор" путем выбора одного или более пунктов;
3. ограничить операцию "выбор", удалив некоторые из вариантов, но оставив два или более.

Операция "уточнение"

Операция "уточнение" может быть выполнена по отношению к любому требованию. Разработчик ПЗ/ЗБ выполняет уточнение путем изменения требования.

1. *Первое* правило по отношению к уточнению состоит в том, чтобы ОО, удовлетворяющий уточненному требованию, также удовлетворял неуточненному требованию в контексте ПЗ/ЗБ (т.е. уточненное требование должно быть "более строгим", чем исходное требование). Если уточнение не удовлетворяет этому правилу, то результирующее уточненное требование считается расширенным требованием и будет рассматриваться как таковое.
2. *Второе* правило по отношению к уточнению состоит в том, что уточнение должно быть связано с исходным компонентом.

Зависимости между компонентами и

Между компонентами могут существовать зависимости. Зависимости возникают, когда компонент не самодостаточен и предполагает наличие другого компонента для обеспечения функциональных возможностей безопасности или доверия к безопасности.

Функциональные компоненты обычно имеют зависимости от других функциональных компонентов, также как некоторые компоненты доверия в могут иметь зависимости от других компонентов. Не исключено также наличие зависимостей расширенных функциональных компонентов от компонентов доверия или наоборот.

Зависимости между компонентами

Другими словами, если компонент А имеет зависимость от компонента Б, это означает, что когда ПЗ/ЗБ содержит требование безопасности, основанное на компоненте А, ПЗ/ЗБ должен также содержать одно из следующего:

1. требование безопасности, основанное на компоненте Б;
2. требование безопасности, основанное на компоненте, более высоком по иерархии по отношению к Б;
3. обоснование, почему ПЗ/ЗБ не содержит требования безопасности, основанного на компоненте Б.

Расширенные компоненты

Существуют цели безопасности для ОО, которые не могут быть преобразованы в функциональные требования безопасности. или существуют требования "третьей стороны" (например, законы, стандарты)

Цели безопасности могут быть выражены на основе компонентов из ИСО/МЭК 15408-2 и/или ИСО/МЭК 15408-3, но только с большими трудностями и/или сложностями. (ISO — международные стандарты)

В обоих случаях от разработчика ПЗ/ЗБ требуется определить собственные компоненты. Эти вновь определенные компоненты называются расширенными компонентами. Точно определенный расширенный компонент необходим для обеспечения контекста и значения расширенных ФТБ или ТДБ, основанных на этом компоненте.