Практическая работа №8

АНАЛИЗ СТРУКТУРЫ ЗАДАНИЯ ПО БЕЗОПАСНОСТИ

Цель работы. Изучить структуру задания по безопасности.

Краткие сведения из теории

Задание по безопасности (Security Target) – совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного объекта оценки.

Обозначения и сокращения:

– ЗБ – задание по безопасности;

– ИТ – информационная технология;

– КСБО – комплекс средств безопасности объекта оценки;

– ОО – объект оценки;

– ПЗ – профиль защиты;

– СБ – средство безопасности;

– УГО – уровень гарантии оценки.

Спецификация заданий по безопасности

1 Общие положения

ЗБ содержит требования безопасности ИТ для конкретного объекта оценки, определяет функциональные и гарантийные меры безопасности, реализация которых обеспечивает соответствие объекта установленным требованиям.

ЗБ является основой для соглашения между разработчиками, экспертами и, если необходимо, заказчиками (потребителями) по характеристикам безопасности объекта и области применения объекта. Лица, заинтересованные в таком задании, не ограничиваются только ответственными за разработку объекта и оценку его безопасности, но к ним также могут быть отнесены ответственные за управление, маркетинг, продажу, инсталляцию, конфигурирование, функционирование и использование объекта.

ЗБ может включать набор требований безопасности или условия соответствия одному или более нескольким ПЗ.

2 Содержание задания по безопасности

2.1 Содержание и представление

Содержание ЗБ должно отвечать требованиям настоящего приложения. ЗБ должно быть представлено в виде документа с минимальным количеством ссылок на другие источники, которые могут оказаться недоступными пользователю ЗБ. Если необходимо, то отдельно представляется

обоснование ЗБ.

Структура ЗБ приведена на рисунке 1. Она используется при разработке структурных элементов ЗБ.

Рисунок 1 – Структура задания по безопасности

2.2 Введение в описание задания по безопасности

Введение в описание ЗБ должно включать следующие структурные

элементы:

а) идентификацию ЗБ, которая должна содержать обозначения и описания, необходимые для идентификации ЗБ и объекта, к которому оно относится;

б) обзор ЗБ, в котором должно быть представлено краткое описание ЗБ. Обзор должен быть достаточно подробным, чтобы потенциальный потребитель объекта мог составить заключение о пригодности объекта для своих целей. Обзор должен быть также удобным для представления в виде отдельного реферата в перечне сертифицированных продуктов;

в) требования соответствия стандарту, в которых должна быть определена степень достоверности, с которой ЗБ соответствует функциональным, гарантийным требованиям или непосредственно ПЗ типового объекта.

2.3 Описание объекта

Описание объекта должно обеспечивать понимание требований его безопасности и давать представление о типе продукта или системы ИТ, а также содержать описание как физических (аппаратных и/или программных компонентов/модулей), так и логических (характеристик ИТ и безопасности объекта) возможностей и областей применения объекта.

Описание объекта представляет данные для его оценки. Информацию, содержащуюся в описании объекта, можно использовать в процессе оценки для выявления несоответствий между политикой, задачами и требованиями безопасности объекта. Если объект представляет продукт или систему, основной функцией которых является безопасность, то этот раздел можно использовать для описания более широкого круга области применения объекта.

2.4 Среда безопасности объекта

Описание среды безопасности объекта должно содержать связанные с безопасностью характеристики среды, в которой будет использоваться объект, и предполагаемый способ эксплуатации объекта.

Оно включает:

а) предположения, которые должны содержать следующие связанные с безопасностью характеристики среды объекта:

1) информацию о предполагаемом порядке использования объекта, в том числе о прикладной области применения, предполагаемой стоимости активов и о возможных ограничениях на использование;

2) информацию о среде, в которой будет использоваться объект, включая вопросы, связанные с КСБО, подбором персонала и внешними связями с другими объектами;

б) угрозы активам, которые исходят из окружающей среды объекта и создают опасность для его работы и против которых требуется защита средствами объекта или его среды.

Угрозы должны быть описаны в понятиях: источник угроз (нарушитель), атака и актив, который подвергается атакам; источники угроз – в понятиях: квалификация, используемый ресурс и мотивация;

атаки – в понятиях: методы атак, используемые уязвимые места и возможности для атаки.

Если задачи безопасности объекта выводятся только из политики безопасности организации и предположений, то структурный элемент «Угрозы» в ЗБ можно опустить;

в) политику безопасности организации, которая должна определять и при необходимости объяснять разделы политики безопасности или правила, которым должен соответствовать объект. Каждый раздел политики следует представлять в форме, позволяющей использовать ее для формулирования

четких задач безопасности ИТ.

Если задачи безопасности объекта выводятся только из угроз и предположений, то структурный элемент «Политика безопасности организации» в ЗБ можно опустить.

Для территориально разнесенного объекта анализ среды безопасности объекта (предположений, угроз, политики безопасности) должен производиться отдельно для каждого района расположения объекта и условий его эксплуатации.

2.5 Задачи безопасности

Задачи безопасности должны отражать намерение противостоять всем установленным угрозам и/или поддерживать принятую политику безопасности и предположения. Различают следующие типы задач безопасности:

а) задачи безопасности для объекта, которые должны быть четко сформулированы для того, чтобы их решение позволило противостоять угрозам средствами безопасности объекта и/или поддерживать политику безопасности организации, которой должен следовать объект;

б) задачи безопасности для среды, которые должны быть четко сформулированы для того, чтобы их решение позволило противостоять угрозам средствами безопасности объекта и среды и/или поддерживать политику безопасности организации, которой должен следовать объект. Формулировки задач безопасности для среды могут повторять (частично или полностью) предположения в описании среды безопасности объекта.

Примечание – Если противодействие угрозе или проведение политики безопасности возлагается на объект и его среду, то соответствующие задачи безопасности формулируются для объекта и среды.

2.6 Требования безопасности информационных технологий

Требования безопасности ИТ должны задаваться следующим образом:

а) в разделе «Требования безопасности объекта» должны быть представлены функциональные и гарантийные требования безопасности, которым должен отвечать объект, и заключение о соответствии требований задачам безопасности объекта.

Требования безопасности объекта включают в себя:

1) функциональные требования безопасности объекта, которые должны задаваться как функциональные компоненты по СТБ 34.101.2.

В тех случаях, когда по условиям безопасности требуется выделить различные аспекты одного и того же требования (например, при идентификации нескольких типов пользователей), можно повторно (т. е. применив операцию итерации) использовать один и тот же компонент.

Если гарантийные требования объекта включают компонент AVA_SOF.1 «Оценка стойкости средства обеспечения безопасности», то в описании функциональных требований безопасности объекта должен устанавливаться минимальный уровень стойкости для СБ, реализованных вероятностными методами или методами перестановок (например, с помощью паролей или хэш-функций).

КСБО должен обладать, по крайней мере, этим уровнем стойкости. Имеется три уровня стойкости СБ:

базовый, средний и высокий. Выбор уровня стойкости производится в соответствии с задачами безопасности объекта. При решении определенных задач безопасности допускается для реализации некоторых функциональных требований выбирать специальную меру стойкости СБ.

При выборе уровня стойкости СБ (компонент AVA_SOF.1 «Оценка стойкости средства обеспечения безопасности» необходимо установить, соответствуют ли выбранные уровни стойкости отдельных СБ и объекта в целом общему минимальному уровню стойкости;

2) гарантийные требования безопасности объекта, которые должны задаваться в виде одного из УГО, возможно, усиленного за счет гарантийных компонентов по СТБ 34.101.3. Усиление УГО в ЗБ может осуществляться также за счет включения дополнительных гарантийных компонентов, не входящих в СТБ 34.101.3;

б) в разделе «Требования безопасности для среды ИТ» должны содержаться требования безопасности, которым должна соответствовать среда ИТ объекта. Если объект независим от среды ИТ, то этот раздел можно опустить. Требования безопасности, не относящиеся к среде ИТ, но часто используемые на практике, могут не включаться в ЗБ, так как они не связаны непосредственно с реализацией объекта;

в) перечисленные ниже условия формирования требований безопасности в равной степени относятся как к функциональным и гарантийным требованиям безопасности объекта, так и к его среде:

1) требования безопасности ИТ должны быть представлены в виде

компонентов требований безопасности по СТБ 34.101.2 и СТБ 34.101.3. Если компоненты требований безопасности по СТБ 34.101.2 и СТБ 34.101.3 не применимы для ЗБ объекта или этих компонентов недостаточно, то недостающие требования безопасности задаются независимо от компонентов требований по СТБ 34.101.2 и СТБ 34.101.3;

2) дополнительные функциональные и гарантийные требования безопасности должны быть четко и однозначно сформулированы, чтобы не возникало трудностей при их оценке и при проверке степени их реализации. Образцом уровня детализации и способа представления требований безопасности может стать представление функциональных или гарантийных требований по СТБ 34.101.2 и СТБ 34.101.3;

3) должны быть использованы все необходимые операции для конкретизации требований безопасности с тем, чтобы обеспечить соответствие требований задачам безопасности. Все разрешенные операции над компонентами требований должны быть завершены.

4) должны быть удовлетворены все зависимости между требованиями безопасности объекта.

Указанные зависимости могут быть удовлетворены за счет включения необходимых требований в перечень требований безопасности объекта либо среды.

2.7 Общая спецификация объекта

Структурный элемент «Общая спецификация объекта» должен содержать описание КСБО и мер гарантии ОО, отвечающих требованиям безопасности. В ряде случаев функциональная информация, являющаяся частью общей спецификации объекта, идентична информации, содержащейся в требованиях семейства ADV_FSP «Функциональная спецификация».

Общая спецификация объекта включает:

а) описание комплекса средств безопасности объекта, которое должно включать перечень СБ ИТ и определять, каким образом эти средства реализуют функциональные требования безопасности объекта. В описании должно быть взаимное соответствие СБ и требований с четким указанием, какие средства соответствуют каким требованиям, а также подтверждение того, что все требования удовлетворены.

Каждое СБ должно обеспечивать реализацию, по крайней мере, одного функционального требования безопасности объекта. Это достигается тем, что:

1) СБ ИТ определяются неформальным способом на уровне описания, необходимом для понимания их назначения;

2) механизмы безопасности должны соответствовать СБ с тем, чтобы можно было определить, какие механизмы безопасности используются для реализации каждого средства;

3) если в состав гарантийных требований безопасности объекта входит компонент AVA_SOF.1 «Оценка стойкости средства обеспечения безопасности», то должны быть указаны СБ ИТ, реализованные с помощью вероятностных методов или метода перестановок (например, с помощью пароля или хэш-функции). Возможность нарушения механизма безопасности таких средств посредством преднамеренного или случайного воздействия имеет непосредственное отношение к безопасности объекта.

Необходимо провести анализ стойкости этих средств. Стойкость каждого средства должна быть оценена как базовая, средняя или высокая или как введенная дополнительно мера стойкости. Результаты оценки стойкости используются экспертом для проверки адекватности и корректности реализации требуемого уровня стойкости;

б) описание мер гарантии, обеспечиваемые установленными гарантийными требованиями. Меры гарантии должны быть отражены таким образом, чтобы было понятно, какие меры участвуют в реализации требований.

Меры гарантии могут быть отражены в ЗБ также путем ссылки на соответствующие планы обеспечения качества, жизненного цикла или управления.

2.8 Требования соответствия профилям защиты

В ЗБ может содержаться требование обеспечения соответствия объекта требованиям безопасности одного или нескольких ПЗ. Эта дополнительная часть ЗБ включает разъяснения, подтверждения и иные вспомогательные материалы. Требование соответствия объекта ПЗ может повлиять на форму описания и содержание той части ЗБ, в которой приведены задачи и требования безопасности объекта. Это влияние может быть сведено к следующим случаям:

а) при отсутствии в ЗБ требований на соответствие ПЗ задачи и требования безопасности объекта представляются так, как приведено в 2.5 и 2.6 (при этом требования, приведенные в ПЗ, не включаются в ЗБ);

б) при наличии в ЗБ только требований соответствия требованиям безопасности, приведенным в ПЗ, то достаточно ссылки на ПЗ, чтобы определить и оценить задачи и требования безопасности объекта (при этом не требуется приводить повторно описание ПЗ);

в) если в ЗБ есть требование не только обеспечить соответствие ПЗ, но и провести более глубокую детализацию требований, приведенных в ПЗ, то в ЗБ должно быть показано, что требование детализации удовлетворено.

Такая ситуация обычно возникает, когда ПЗ содержит незавершенные операции. В этом случае в ЗБ может быть сделана ссылка на ПЗ, но дополнительные детализированные требования приводятся в ЗБ. При определенных обстоятельствах, когда дополнительные детализированные тре-

бования являются существенными и их реализация обязательна, то необходимо в ЗБ повторно привести описание требований, приведенных в ПЗ;

г) если в ЗБ есть требование не только обеспечить соответствие ПЗ, но и расширить перечень задач и требований безопасности, то в разделах ЗБ, где имеются ссылки на ПЗ, должны быть приведены дополнительные задачи и требования безопасности. Если дополнительные задачи и требования безопасности являются существенными, то необходимо в ЗБ повторно привести описание задач и требований безопасности, приведенных в ПЗ.

В настоящем стандарте не рассматриваются случаи, когда в ЗБ требуется лишь частичное его соответствие ПЗ.

В стандарте не устанавливается никаких правил описания в ЗБ задач и требований безопасности, приведенных в ПЗ, или ссылок на них. Основополагающим является требование, чтобы содержание ЗБ было полным, ясным, исключало различные толкования, позволяло провести оценку ЗБ, являлось бы приемлемой основой для оценки объекта и допускало сравнение с любым нужным ПЗ.

Если имеется требование соответствия ЗБ нескольким ПЗ, то соответствующий раздел ЗБ должен для каждого ПЗ включать следующие данные:

а) ссылку на профиль защиты, на основе которой определяется тот ПЗ, которому должно соответствовать ЗБ, вместе со всеми дополнительными материалами, которые могут усилить условие соответствия. Правильно сформулированное условие соответствия (после усиления) подразумевает, что объект отвечает всем требованиям ПЗ;

б) уточнение профиля защиты, определяющее формулировки задач и требований безопасности объекта, которые удовлетворяют допустимым операциям ПЗ или проводят дальнейшую детализацию задач и требований безопасности, т. е. уточняют требования безопасности;

в) дополнение профиля защиты, определяющее формулировки задач и требований безопасности объекта, которые дополняют задачи и требования безопасности, приведенные в ПЗ.

2.9 Обоснование задания по безопасности

Обоснование ЗБ должно подтвердить, что:

а) ЗБ содержит полную и взаимоувязанную совокупность требований безопасности;

б) разработанный в соответствии с заданными требованиями объект будет обладать эффективным набором средств обеспечения безопасности ИТ в среде безопасности;

в) общая спецификация объекта отражает заданные требования.

Обоснование также должно подтвердить соответствие ЗБ каждому ПЗ, указанному в ЗБ.

В обоснование должны входить:

а) обоснование задач безопасности, которое подтверждает, что сформулированные задачи безопасности охватывают все указанные аспекты среды безопасности объекта и верно отражают их;

б) обоснование требований безопасности, которое подтверждает, что заданная совокупность требований безопасности объекта и его среды отвечает задачам безопасности.

При обосновании требований безопасности необходимо показать, что:

1) совокупность компонентов функциональных и гарантийных требований объекта и его среды обеспечивает выполнение установленных задач безопасности объекта;

2) набор требований безопасности образует единую и взаимоувязанную совокупность требований;

3) выбор требований безопасности обоснован.

Специальное обоснование необходимо при задании требований, не содержащихся в СТБ 34.101.2 и СТБ 34.101.3, а также в случае неудовлетворенных зависимостей;

4) выбор уровня стойкости СБ в ПЗ обоснован.

Требования к стойкости СБ должны быть согласованы с задачами безопасности объекта;

в) обоснование общей спецификации объекта, которое должно показывать, что СБ и гарантийные меры отвечают требованиям безопасности объекта.

При обосновании общей спецификации объекта необходимо показать, что:

1) СБ реализуют функциональные требования безопасности объекта;

2) требования к стойкости СБ обоснованы либо такие требования не предъявляются;

3) подтверждено условие соответствия принятых мер гарантии гарантийным требованиям.

Уровень детализации обоснования общей спецификации должен соответствовать уровню детализации описания КСБО.

г) обоснование требования соответствия профилям защиты, которое содержит объяснения различий между задачами и требованиями безопасности, представленными в ЗБ и в каждом ПЗ, соответствие которым должно быть обеспечено. Если в ЗБ отсутствует требование соответствия ПЗ или задачи и требования безопасности, представленные в ЗБ и в ПЗ, совпадают, то этот раздел в ЗБ можно опустить.

Обоснование должно предоставляться по желанию потребителей ЗБ.

Порядок выполнения работы

1 Ознакомится со структурой задания по безопасности.

2 Составить план задания по безопасности для объекта оценки из предыдущих практических занятий или по заданию преподавателя.

3 Сделать выводы.

Содержание отчета

1 Цель работы.

2 План задания по безопасности объекта оценки.

3 Вывод по работе.

Контрольные вопросы

1 Серия стандартов Республики Беларусь 34.101.

2 Что такое задание по безопасности?

3 Структура задания по безопасности.