УДК 004.05

Е.И. Неткачёва[1], В.С. Харченко[2]

[1]*Таврический национальный университет им. В.И. Вернадского, Симферополь*
[2]*Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков*

ДОКАЗАТЕЛЬСТВО И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ФОРМАЛЬНЫХ НОТАЦИЙ

Рассмотрены современные подходы к построению доказательства безопасности с использованием формальных нотаций. Представлена концепция обоснований безопасности, гарантии и доверия, описана организация процесса разработки и структура результирующих отчетов по безопасности. Рассмотрены и проанализированы три наиболее распространенные нотации для представления обоснований: нотация Тулмина, Ascad и GSN, с подробным описанием основных элементов и схематичным представлением и анализом моделей аргументов этих нотаций.

Ключевые слова: *обоснование безопасности, обоснование гарантии, обоснование доверия,, нотация Тулмина, ASCAD, нотация структурирования целей.*

Введение

Сферы технической деятельности приобретают всё большее значение в современном мире. Внедрение информационных технологий, автоматизация процессов производства, компьютеризация различных отраслей человеческой деятельности, помимо новых возможностей, представляют и новые угрозы для человека, общества, окружающей среды. В связи с этим чрезвычайно актуальной является задача оценки уровня безопасности систем и проведения убедительного формального доказательства.

Одним из актуальных направлений исследований в настоящее время является методология построения обоснований безопасности, гарантии и доверия с использованием формальных нотаций. Значительный вклад в развитие этой методологии внесли работы западных ученых П. Бишопа [1 – 3], Р. Блумфилда [4, 5], Т. Келли [6, 7], Р. Хокинса [8 – 11], Я. Горски [12, 13] и др.

В данной работе рассматриваются современные подходы к проведению доказательства безопасности и основные формальные нотации, которые используются при доказательстве.

Важной задачей работы является обзор англоязычных работ, т.к. в настоящее время русскоязычных публикаций в этой области крайне мало.

К сожалению, русская терминология многих понятий еще не устоялась, поэтому при переводе английских терминов на русский язык встречались некоторые трудности.

Для максимальной ясности в табл. 1 представлен список английских прообразов и выбранные авторами переводы некоторых основных терминов, которые используются в данной работе.

Таблица 1

Перевод основных терминов

Safety Case	Обоснование безопасности
Assurance Case	Обоснование гарантии
Trust Case	Обоснование доверия
GSN	Нотация структурирования целей
ASCAD	Нотация ASCAD (аббр. разработка обоснования безопасности Аделарда)
Claim	Утверждение
Warrant	Основание
Rebuttal	Опровержение
Backing	Подкрепление
Evidence	Доказательство
Arguments	Аргументы
Qualifier	Квалификатор
Inference rule	Логический вывод
Goal	Цель
Strategy	Стратегия
Solution	Решение
Context	Контекст
Links	Ссылки
Reference	Указатель
Justification	Обоснование

1. Понятие Safety Case методологии

Одним из важнейших направлений в области безопасности является развитие использование Safety Case методологии. Данная методология представляет собой систему принципов, методов, методик и программных средств, направленных на:

– исследование систем, критичных к безопасности;

– минимизацию рисков безопасности и коммерческих рисков системы;

– выявление фактов, данных, аргументов, свидетельств, позволяющих построить убедительное доказательство того, что исследуемая система действительно является безопасной и будет оставаться таковой при определенном функционировании в заданных условиях эксплуатации на протяжении всего жизненного цикла.

Результатом такого анализа является построение комплексного обоснования безопасности – Safety Case документа.

Существует множество определений понятия Safety Case. Классическим считается определение [4], данное специалистами компании Adelard и исследовательского центра CSR (университет City University London), которые являются идеологами данной методологии: обоснование безопасности – это документально оформленная совокупность доказательств, представляющих веское и убедительное обоснование того, что система является достаточно безопасной при заданном использовании в заданных условиях эксплуатации.

Еще одним из вариантов, представляющих интерес, является развернутое определение, которое было дано в руководстве по системе управления безопасностью судов министерства обороны Великобритании U.K. Ministry of Defense Ship Safety Management System Handbook [14]: обоснование безопасности – это полный структурированный комплект документации о безопасности, направленный на то, чтобы безопасность определенной системы или оборудования можно было продемонстрировать на основе следующего:

– организация и техника безопасности;

– анализ безопасности;

– соблюдение стандартов и нормативов;

– испытания на соответствие техническим условиям;

– аудиты;

– проверки;

– обратная связь;

– меры, принятые для безопасного использования, включая меры, принимаемые в случае критической ситуации.

Из этих двух определений следует, что Safety Case – это прежде всего документ, предоставляющий доказательство безопасности исследуемого продукта или системы.

Однако в широком смысле понятие Safety Case включает в себя также логическую составляющую и в связи с этим употребляется часто для обозначения особого подхода к организации безопасности, который включает разработку и использование комплек-

са мероприятий для улучшения безопасности программы или системы, с последующим представлением обоснования безопасности в виде документа.

Рекомендации стандартов предлагают различную структуру документов по обоснованию безопасности. Следующий список иллюстрирует наиболее типичные заголовки пунктов [6]:

– область применения;
– описание системы;
– системные опасности;
– требования безопасности;
– оценка риска;
– меры по контролю и снижению степени риска;
– анализ безопасности/испытание на безопасность;
– система управления безопасностью;
– обоснование процесса разработки;
– заключение и выводы.

2. Организация процесса обоснования безопасности

Разработка элементов обоснования безопасности не является простым поэтапным процессом, так как основные процессы взаимодействуют друг с другом и повторяются в процессе разработки и в то время, как уровень сложности (иерархии) компонентов системы изменяется.

Для реализации обоснования безопасности необходимо принять во внимание и выполнить следующие действия [15]:

– составить точный ряд утверждений относительно системы;
– определить подтверждающие доказательства;
– предоставить ряд аргументов в пользу безопасности, которые связывают между собой претензии с доказательствами;
– детализация, основанная на анализе и оценке;
– разъяснить предположения и суждения, лежащие в основе аргументов;
– предоставить различные точки зрения и уровни детализации.

Существует четыре элемента, из которых, в различных комбинациях, можно создать обоснование безопасности, необходимое для реального проекта. Эти элементы:

– предварительный;
– архитектурный;
– реализация;
– эксплуатация и установка.

Масштаб и характер проекта будет определять количество и тип необходимых элементов обоснования безопасности. Внутри системы и отдельных частей обоснования безопасности может быть рекурсивная структура с многочисленными предварительными и архитектурными элементами.

Характеристики элементов обоснования безопасности таковы, независимо от того, рассматривается ли новая или уже существующая система.

Предварительный элемент обоснования безопасности:

– устанавливает контекст системы, указывающий, предназначено ли обоснование безопасности для полной системы или компонента внутри системы, и фазу цикла осуществления проекта;
– устанавливает требования безопасности, атрибуты уровня разработки и интерфейсы для анализа безопасности системы;
– определяет эксплуатационные требования и ограничения, такие как уровни технического обслуживания, время восстановления.

Архитектурный элемент обоснования безопасности определяет**:**

– архитектуру системы или подсистемы и создает компромиссы между проектированием системы и опциями для обоснования безопасности;
– предположения, которые необходимо подтвердить, и доказательства, которые должны быть предусмотрены в сложных обоснованиях безопасности;
– насколько проектирование соответствует предварительным операционным и инсталляционным аспектам обоснования безопасности (например, через ремонтопригодность, модифицируемость и простоту использования).

Причиной для выделения архитектурного обоснования безопасности является важное значение, которое имеет хорошая архитектура и грамотное проектирование в обеспечении безопасности. К сожалению, этой областью проектирования и стандартов обеспечения безопасности часто пренебрегают.

Элемент реализации обоснования безопасности:

– предоставляет обоснование того, что конструктивная концепция архитектурного обоснования безопасности была реализована и что действительные конструктивные особенности и процесс разработки прдоставляют доказательства того, что требования безопасности удовлетворены;
– устанавливает дополнительные предположения по эксплуатации и техническому обслуживанию, и приводит подробное описание того, как соблюдать эксплуатационные требования.

Элемент эксплуатации и установки обоснования безопасности:

– дополняет деталями требования по эксплуатации и поддержке, установленные в реализации обосновании безопасности;
– определяет последовательность операций системы безопасности, установленной в предварительном обосновании безопасности или архитектурном обосновании безопасности;

– для коммерческой предразработанной программной системы “с полки”, обоснование безопасности будет включать в себя обоснование безопасности особой конфигурации, проблемы человеческого фактора, такие как требования кадрового обеспечения и уровни компетенции, подготовка операторов и специалистов по техническому обслуживанию и ремонту, оборудование для долгосрочной поддержки.

Обоснование безопасности как документ будет также регистрировать и анализировать случаи несоблюдения исходных требований по безопасности.

3. Анализ основных нотаций, применяемых при обосновании безопасности

3.1. Модель аргументации Тулмина

Система обозначений Тулмина [16] описывает схему структуру типового аргумента (рис. 1).

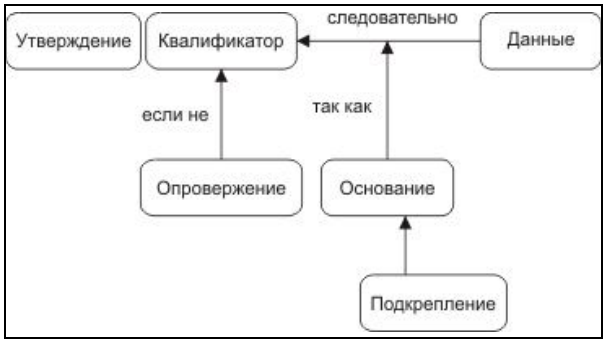


Рис. 1. Модель аргументации Тулмина

Эта схема состоит из шести взаимозависимых компонентов, которые можно определить следующим образом:

– **утверждение** – определенное заключение, которое нужно доказать, некоторые утверждения о рассматриваемом свойстве системы или ее подсистемы (требование, свойство, которым должна обладать система и т.п.);

– **данные** – факты, на которые ссылаются в качестве основания утверждения;

– **основание** – причина, по которой следует принять представляемые доказательства, обоснование того, что факты действительно подтверждают утверждение. Оно фактически связывает данные и другие обоснования с утверждением;

– **подкрепление** – данные, предназначенные для удостоверения утверждения, выраженного в основании, подкрепление дает дополнительную поддержку для основания и должно быть представлено тогда, когда само по себе основание не является достаточно убедительным;

– **квалификатор** – степень уверенности в истинности рассматриваемого утверждения;

– **опровержение** – контраргументы, которые могут быть использованы для опровержения истинности утверждения, а также ограничения или определенные условия, при которых утверждение может не выполняться.

Существуют также понятия обоснованности и правильности аргументов.

Обоснованность аргумента – это корректность используемого обоснования. Обоснование должно быть логически верным, а используемые данные – релевантными (они должны влиять на заключение, т.е. утверждение) и пригодными (достоверность данных должна предполагать истинность заключения).

Аргумент считается **правильным**, если он является обоснованным и все данные или предположения, на которые он опирается, являются истинными.

3.2. Анализ Ascad нотации

ASCAD – это название нотации, представляющее собой аббревиатуру, которая расшифровывается как разработка обоснования безопасности компании Аделард. Нотация ASCAD была разработана, как часть методологии обоснования безопасности Аделарда. Ее основной идеей для представления аргументной структуры является мотив «утверждения-аргументы-доказательства» (рис. 2).

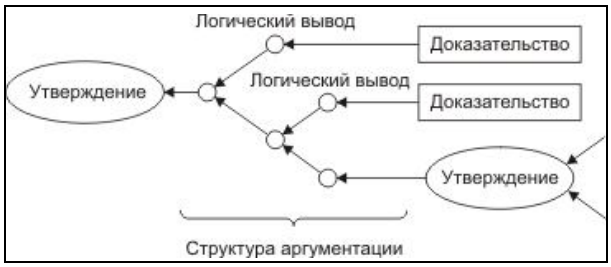


Рис. 2. Модель аргументации ASCAD

Основными элементами структуры являются [15]:

– **утверждения** относительно свойства системы или подсистемы;

– **доказательства**, используемые в качестве основания аргументов безопасности. Это могут быть факты (например, основанные на установленных научных принципах и предварительном исследовании), предположения, или дополнительные утверждения, полученные из подаргументов более низкого уровня;

– **аргументы**, связывающие между собой доказательства и утверждения, могут быть детерминистическими, вероятностными или качественными;

– **логический вывод** – механизм, предоставляющий трансформационные правила для аргументации.

Также является возможным иметь два (или более) независимых аргумента, обосновывающих одно и то же утверждение.

Следует обратить внимание, что доказательством может быть дополнительное утверждение, представленное вспомогательным обоснованием

безопасности. Иными словами, обоснованием утверждения может быть ряд дополнительных утверждений нижнего уровня, и можно продемонстрировать утверждение верхнего уровня, показывая, что утверждения нижнего уровня обоснованы, и доказывая, что все аргументы являются достоверными. Это означает, что может иметь место относительно простая аргументация верхнего уровня, опирающаяся на структуру вспомогательных обоснований безопасности нижнего уровня.

Для обоснования утверждений могут быть использованы различные типы аргументации:

– детерминистическое применение заранее установленных правил для установления истинности или ложности утверждения (принимая во внимание исходные предположений), например, формальное доказательство соответствия спецификации, или демонстрация требования безопасности (такого как анализ времени выполнения или исчерпывающее тестирование логики);

– вероятностное количественное статистическое обоснование для установления численного уровня (например, средняя наработка до отказа, среднее время восстановления, проверка надежности);

– качественное соблюдение норм, имеющих косвенную связь с требуемыми атрибутами (например, соблюдение стандартов системы управления качеством, навыки и опыт персонала).

Выбор аргумента будет зависеть от имеющихся доказательств и типа утверждения. Например, утверждения относительно надежности обычно обосновывают статистическими аргументами, в то время как другие претензии (например, относительно ремонтопригодности) могут опираться на более качественные аргументы, такие как соблюдение норм и правил.

Кроме того, все аргументы должны быть устойчивыми, т.е. они должны быть достоверными, даже при наличии неточностей и ошибок. Например, два независимых аргумента могут быть использованы для обоснования утверждения верхнего уровня относительно данной системы. И наоборот, если существует две независимых системы, которые могут обеспечить безопасность, возможно, понадобится только один аргумент для каждой.

Как правило, убедительность аргумента будет зависеть от уровня целостности, связанного с определенной системой. На самом высоком уровне целостности можно ожидать два независимых аргумента для одной системы, независимо от существования другой системы.

3.3. Обзор графической GSN нотации

GSN или нотация структурирования целей это графическая аргументативная система обозначений, разработанная в Йоркском Университете. Нотация структурирования целей подробно представляет отдельные элементы любого аргумента безопасности (требования, утверждения, доказательства и контекст) и (возможно, более существенно) отношения, существующие между этими элементами (т.е. как отдельные требования обоснованы определенными утверждениями, как утверждения обоснованы доказательствами и предполагаемый контекст, который определен для аргумента). Аргументы, задокументированные с помощью GSN нотации, могут помочь предоставить гарантию для критических свойств систем, услуг и организаций (такие, как свойства безопасности).

Цель GSN – документально обосновать, как цели (выводы аргумента) обосновываются подцелями (предпосылками аргумента). Затем можно показать, как эти подцели обоснованы последующими вспомогательными целями.

Когда существуют доказательства для обоснования достоверности заявленной цели, это может быть документировано путем предоставления решения в GSN.

Документируя как цели обоснованы подцелями, может быть полезным документировать этап обоснования – т.е. природу аргумента, который соединяет цель с ее подцелями. Это делается в GSN путем документирования связующей аргументативной стратегии.

Документируя цель, может быть также важным захватить контекст, в котором данное утверждение должно быть интерпретировано. Это делается в GSN путем документирования контекста.

Цели, стратегии, решения и контекст являются основными элементами GSN.

Когда элементы GSN соединяются вместе, они формируют собой так называемую «целеориентированную структуру». Целеориентированные структуры документируют цепь рассуждений по аргументу (через видимое разделение заявленных целей и описание аргументативных стратегий), как этот аргумент обоснован доказательством (через решения), и четко захватывают контекст, в котором выдвигаются заявленные цели аргумента [17].

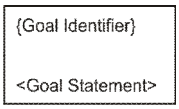
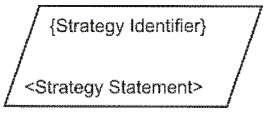
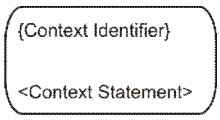
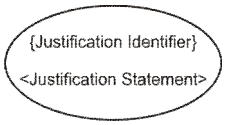
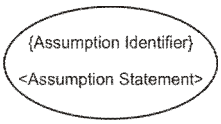
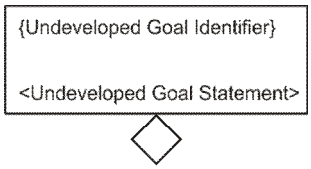
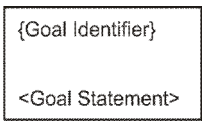
Определение и графическое изображение основных символов GSN и связей представлены в табл. 2.

3.4. Модель аргументации Trust-IT

Существует еще один подход, который предлагает взглянуть на вопрос исследования системы в более широком плане и рассмотреть дополнительные аргументные структуры, которые могут использоваться для демонстрации свойств, отличных от безопасности. Этот подход, а также связанная с ним методология Trust-IT, были предложены и продолжают развиваться исследователями Гданьского технологического университета. Вместо понятия обоснования безопасности в данном подходе используется понятие обоснование доверия.

Таблица 2

Основные элементы нотации структурирования целей

	Цель, графически изображенная в виде прямоугольника, представляет утверждение, формирующее часть аргументации.
	Стратегия, изображенная в виде параллелограмма, описывает природу логического вывода, существующего между одной или несколькими целями и другой целью.
	Решение, изображенное в виде круга, представляет ссылку на доказательства.
	Контекст, изображенный слева, представляет контекстуальный артефакт. Это может быть ссылка на контекстуальную информацию или утверждение.
	Обоснование, изображенное в виде овала, с буквой «J» справа внизу, представляет логическое обоснование.
	Предположение, изображенное в виде овала с буквой «A» справа внизу, представляет намеренно необоснованное утверждение.
	Неразработанный объект, изображенный в виде ромба, указывает на то, что ряд аргументов не был разработан. Это может относиться к целям (как представлено ниже) и стратегиям.
	Неразработанная цель, изображенная в виде прямоугольника с ромбом – символом неразработанного объекта внизу в центре, представляет утверждение, намеренно неразработанное в аргументации.
	Логическое обоснование, изображенное в виде стрелки с заливкой, показывает логическую (представляющую собой явный вывод между целями аргумента) или очевидную (представляющую собой явную связь между целью и доказательством, обосновывающим цель) связь. Допустимые связи: цель-цель, цель-стратегия, цель-решение, стратегия-цель.
	Контекстная связь, изображенная в виде стрелки без заливки, показывает контекстуальную связь элементов. Допустимые связи: цель-контекст, цель-предположение, цель-обоснование, стратегия-контекст, стратегия-предположение и стратегия-обоснование.
	Цель, графически изображенная в виде прямоугольника, представляет утверждение, формирующее часть аргументации.

Обоснование доверия – это документально подтвержденная база, предоставляющая достаточно убедительное (с определенной точки зрения) обоснование заданной совокупности утверждений (относительно свойств объекта, рассматриваемого для данной цели в данных условиях) с целью показать, что они заслуживают доверия [13].

Точки зрения, указанные в определении, представляют собой заинтересованность наблюдателей (заинтересованные лица, аудиторы и т.д.) в рассматриваемом объекте (система, организация и т.д.). Указанная документально подтвержденная база может включать себя любое доказательство и обоснование, и представляется в качестве аргументной структуры.

Горски также положил начало созданию методологии Trust-IT для разработки обоснования безопасности на основании системы обозначения Тулмина, рассмотренной выше. Это одна из современных методологий, которая также имеет инструментальную поддержку в виде приложения Trust-IT, созданным для разработки обоснований доверия и их применения в различных ситуациях.

Инфраструктура Trust-IT состоит из трех компонентов:

– **прикладной компонент** – объясняет возможные варианты использования обоснований доверия;

– **методологический компонент** – объясняет, как разработать и вести обоснования достоверности, определяет язык разработки обоснований доверия, синтаксис, семантику и образцы типичных аргументов обоснований доверия, а также бизнес-процессы и процедуры, имеющие отношение к сценариям применения;

– **инструментальный компонент** – предоставляет обоснование для всестороннего использования двух других компонентов.

Структура модели аргумента Trust-IT представлена на рис. 3.

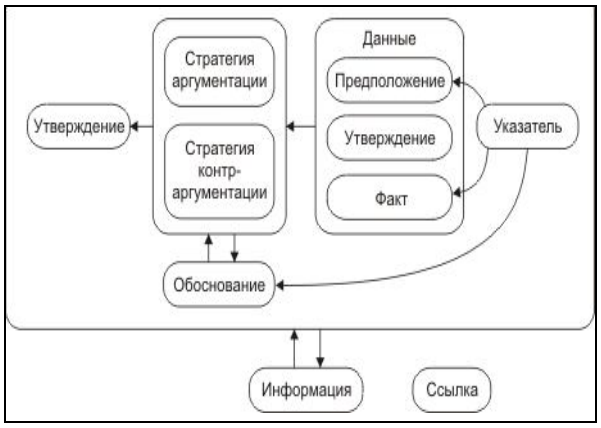


Рис. 3. Структура модели аргумента Trust-IT

Краткое описание узлов представлено ниже:

– **утверждение** – предложение, которое выражает необходимое свойство, каждое утверждение требует дальнейшего обоснования, оно дополняется четким и ясным аргументом;

– **стратегия аргументации** – основная идея о том, как продемонстрировать заключение и каковы критерии отбора данных; утверждение может иметь более одной аргументной стратегии, при этом они предоставляют независимые аргументы заключения;

– **стратегия контраргументации** – основная идея, на которой основывается опровержение обоснованного утверждения; ее можно считать аргументной стратегией для отрицания заключения; утверждение может иметь большое количество контраргументных стратегий; оно также может иметь аргументные стратегии вместе с контраргументными стратегиями;

– **обоснование** – отношение между данными и полученным выводом, которое объясняет, почему при заданных обстоятельствах необходимо или надлежит сделать определенный вывод, если установленные данные или предположения действительно имеют место;

– **предположение** – исходное допущение без дальнейшего обоснования; предположение представляет свойство, не зависимое от того, кто предоставляет обоснование доверия;

– **факт** – утверждение или констатация проверенной информации о том, что нечто является правдой или произошло; это может быть очевидная информация или же информация, основанная на внешних по отношению к обоснованию доверия источниках;

– **указатель** – связь с внешним по отношению к данному обоснованию доверия миром, которая может указывать на любой идентифицируемый внешний объект, которым на практике обычно является объект, на который указывает URL-адрес; с помощью указателей можно объединять объекты, которые содержат доказательства, имеющие отношение к аргументу обоснования доверия;

– **информация** – дополнительная информация, не являющаяся частью аргумента.; ее можно поместить в обоснование доверия, она содержит пояснительную информацию, которая может помочь понять значение обоснования доверия, или помогает организовать структуру обоснования доверия;

– **ссылка** – внутренний указатель, направленный от одного элемента обоснования доверия к другому; используя ссылки, можно избежать древовидной структуры обоснования доверия и сделать ее в виде направленного ациклического графа.

Утверждения и обоснования могут быть продемонстрированы путем использования других утверждений. Это значит, что структура может расти рекурсивно. Таким образом, обоснования доверия могут быть разработаны путем предоставления более детальных аргументов для утверждения и некоторых обоснований, до тех пор, пока они не будут полностью подтверждены.

Аргументная модель может быть применена для представления как формального вывода, так и неформальной аргументации. Она предоставляет способы представления аргументов на основе высокоформализованного анализа, равно как и неопределенных доказательств и индуктивных выводов, которые часто встречаются в реальных ситуациях [18].

4. Анализ Assurance Case подхода

Понятие гарантии системы определяется как оправданная уверенность в том, что система функционирует, как требутся и свободна от эксплуатационных уязвимостей, намеренно или непреднамерен-

но созданных или добавленных как часть системы в любое время жизненного цикла. Этот идеал отсутствия эксплуатационных уязвимостей обычно на практике не достижим, поэтому программы должны выполнять контроль факторов риска, чтобы уменьшить вероятность и воздействие уязвимостей до приемлемых уровней.

Эта уверенность достигается действиями по обеспечению гарантии системы, которые включают в себя запланированный систематический комплекс многоплановых действий для достижения допустимых уровней гарантии системы и управления рисками эксплуатационных уязвимостей.

Обоснования гарантии системы целесообразны в ситуациях, когда необходим рациональный базис уверенности в продукте.

Обычно это ситуации, требующие гарантированного обеспечения какого-либо свойства или свойств продукта.

Целью обоснования гарантии является предоставление заинтересованным лицам убедительного обоснования того, что особо важные требования по обеспечению надежности соблюдаются в ожидаемых системных условиях. В случае, если выражен ряд утверждений относительно обеспечения надежности системы, эти утверждения следует объединить в системные требования. Обоснование гарантии это ряд утверждений о критических свойствах системы, аргументы, обосновывающие утверждения (включая предположения и контекст) и доказательства, подкрепляющие аргументы.

В проектировании систем действия по разработке и ведению обоснования гарантии создают условия для принятия рациональных решений, таких, чтобы выполнялись только те действия, которые необходимы для предоставления достаточного обоснования (аргументов и доказательств). Планирование обоснования гарантии определяет и обосновывает, какой подход будет выбран (например, выбор языка программирования, выбор доверенных источников) и какие доказательства необходимо собрать, чтобы точно достичь и обосновать необходимый уровень гарантии. Это планирование включает в себя стоимостный и технический компромиссы, а также интеграцию в процесс снижения риска, структуру классификации работ, план-график программы/проекта. Разработка обоснования гарантии проясняет взаимодействие между планом проекта, защитой, функциональностью, стоимостью, безопасностью, надежностью, и другими «-стями», так, чтобы можно было найти соответствующие компромиссы через контроль факторов риска.

В системном проектировании разработка и ведение обоснования гарантии должны быть выполнены как часть определения требований заинтересованных лиц, анализа требований, архитектурного дизайна и процессов контроля факторов риска. Обоснование гарантии служит опорой для эффективной разработки системы и сокращает совокупный риск, применяя различный практический опыт/дисциплины/процессы, чтобы соответствовать приоритетным требованиям по гарантии.

Обязательный минимум таков.

1. Утверждения, аргументы и доказательства обоснования гарантии должны быть релевантными для системы и ее операционной среды.

2. Утверждения обосновываются с помощью аргументов.

3. Данные и доказательства подкрепляют аргументы.

4. Обоснование гарантии должно разрабатываться итерационно, должно быть устойчивым и сохраняться в течение всего жизненного цикла системы как актуализированный документ. Это подразумевает то, что обоснование гарантии должно быть разработано таким образом, чтобы его можно было легко изменять, следует использовать инструментальные средства для его поддержки, а также следует разделять его на небольшие модули, чтобы изменения могли быть локализованы.

5. Обоснование гарантии должно поставляться как часть системы и поддерживаться вместе с поддержкой всей системы.

Обоснование гарантии необязательно должно быть отдельным документом, оно может быть распределено между или включено в уже существующие документы. Даже если существует документ «обоснование гарантии», он обычно содержит много ссылок на другие документы. Независимо от того, как выполнена документация обоснования гарантии, всегда должна быть возможность определить все утверждения обеспечения гарантии, проследить связь утверждений с обосновывающими их аргументами и связь этих аргументов с подкрепляющими их доказательствами.

Например, организация может вести список системных требований, помечая отдельные требования как утверждения обеспечения гарантии, с гиперссылками на аргументы, которые обосновывают, почему система будет соответствовать данному утверждению [19].

Выводы

В работе были описаны и проанализированы концепция и основы методологии Safety Case, представлены наиболее популярные нотации и их модели аргументов, основные принципы построения обоснований безопасности и гарантии.

Проведенный анализ показал, что в последние годы отмечается стойкая тенденция к формализации процесса оценки безопасности, активно развиваются подходы, основанные на формальных нотациях.

В перспективе есть необходимость развивать и совершенствовать существующие модели и методы оценки, разрабатывать более универсальные и гибкие методики для использования в различных системах, а также повышать уровень формализации процесса оценки и обоснования безопасности.

Список литературы

1. Bishop P.G. A Methodology for Safety Case Development / P.G. Bishop, R.E. Bloomfield // Industrial Perspectives of Safety-critical Systems: Proceedings of the Sixth Safety-critical Systems Symposium, Birmingham 1998. London, UK. – Springer-Verlag, 1998.

2. Bishop P.G. The future of goal-based assurance cases / P.G. Bishop, R.E. Bloomfield, A.S.L. Guerra // Proceedings of Workshop on Assurance Cases. Supplemental Volume of the 2004 International Conference on Dependable Systems and Networks. – 2004. – June 2004. – Pp. 390-395.

3. Bishop P.G. The SHIP Safety Case / P.G. Bishop, R.E. Bloomfield // Proc. 14th IFAC Conf. Computer Safety, Reliability and Security. – 1995.

4. R.E. Bloomfield. ASCAD – Adelard Safety Case Development Manual / R.E. Bloomfield, P.G. Bishop C.C.M. Jones P.K.D. Froome // Adelard, 1998. ISBN 0-9533771-0-5.

5. R.E. Bloomfield. Confidence: its role in dependability cases for risk assessment / R.E Bloomfield, B. Littlewood // International Conference on Dependable Systems and Network,Edinburgh, IEEE Computer Society. – 2007.

6. T.P. Kelly. Arguing Safety - A Systematic Approach to Managing Safety Cases / T.P. Kelly // PhD thesis, Department of Computer Science, The University of York,. – 1998.

7. T.P. Kelly. The Goal Structuring Notation - A Safety Argument Notation / T.P. Kelly, R.A. Weaver // Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases. – 2004.

8. Richard Hawkins. A Structured Approach to Selecting and Justifying Software Safety Evidence / Richard Hawkins, Tim Kelly // Proceedings of 5th IET International System Safety Conference. Manchester, UK. – 2010.

9. R. Hawkins. Software safety assurance – what is sufficient / R. Hawkins, T. Kelly // Proceedings of the 4th IET International Conference on System Safety. – 2009.

10. Habli, I. Software safety: relating software assurance and software integrity' / Habli, I., Hawkins, R. and Kelly, T. // Int. J. Critical Computer-Based Systems. – 2010. – Vol. 1, No. 4. –P.364–383.

11. Richard Hawkins. A New Approach to creating Clear Safety Arguments / Richard Hawkins, Tim Kelly, John Knight and Patrick Graydon // Proceedings of 19th Safety Critical Systems Symposium (SSS'11). –2011.

12. Górski J. Trust Case – a case for trustworthiness of IT infrastructures / J. Górski // Cyberspace Security and Defense: Research Issues. – 2005.

13. Gorski J. Trust Case: Justifying Trust / Gorski J., Jarzebowicz A., Leszczyna R., Miler J., Olszewski M // IT Solution, Elsevier, Reliability Engineering and System Safety. – 2005. – Vol.89. – P. 33-47.

14. U.K. Ministry of Defense "JSP 430 - Ship Safety Management System Handbook" / Ministry of Defence. – 1996.

15. ASCAD Adelard Safety Case Development Manual / Adelard. – 2010.

16. S.E. Toulmin. The Uses of Argument" / S.E. Toulmin // Cambridge University Press. – 1958.

17. Draft GSN Standard, version 1.0 / York University. – 2010.

18. Ł. Cyra. A Method of Trust Case Templates to Support Standards Conformity Achievement and As-sessment / Ł. Cyra // Doctoral Dissertation, Gdansk University of Technology, Gdansk, Poland. – 2008.

19. National Defense Industrial Association (NDIA) System Assurance Committee. Engineering for System Assurance. // Arlington, VA: NDIA. –2008.

Поступила в редколлегию 4.10.2011

Рецензент: д-р техн. наук, проф. Б.М. Конорев, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ».

ДОКАЗ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ З ВИКОРИСТАННЯМ ФОРМАЛЬНИХ НОТАЦІЙ

К.І. Неткачова, В.С. Харченко

Розглянуті сучасні підходи до проведення доказу безпеки з використанням формальних нотацій. Представлена концепція обґрунтувань безпеки, гарантії і довіри, описана організація процесу розробки і структура результуючих звітів про безпеку. Приведені та проаналізовані структури трьох найпоширеніших нотацій для створення обґрунтувань: нотацій Тулміна, Ascad і GSN. Надано детальний опис основних елементів та схематичних зображень і аналіз моделей аргументів цих нотацій.

Ключові слова: *обґрунтування безпеки, обґрунтування гарантії, обґрунтування довіри, нотація Тулміна, Ascad, нотація структурування цілей.*

SAFETY ASSURANCE AND TRUST CASES WITH THE USE OF FORMAL NOTATIONS

K.I. Netkachova, V.S. Kharchenko

The modern approaches to demonstrating safety with the use of formal notations are described. The concept of safety, assurance and trust cases are presented, the development process and the structure of a typical safety report are outlined. The structures of the three most common notations for representing safety cases (Toulmin, ASCAD and GSN) are reviewed, with their main elements being thoroughly described and the notation argument models schematically illustrated and analyzed.

Keywords: *Safety case, assurance case, trust case, Toulmin, ASCAD, GSN notations.*