УДК 004.05:681.3.06

И.В. Косенко[1], О.А. Усачёва[2], М.Г. Стадниченко[2]

[1] *Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков*
[2] *Харьковский университет Воздушных Сил имени Ивана Кожедуба, Харьков*

ФОРМАЛИЗАЦИЯ ТРЕБОВАНИЙ ГАРАНТИЙ БЕЗОПАСНОСТИ (В СООТВЕТСТВИИ СО СТАНДАРТОМ ISO / IEC 15408) НА ОСНОВЕ CASE-ПОДХОДА

В статье описывается подход к построению инфраструктуры использования программных стандартов. Рассмотрены современные подходы к формализации требований гарантий безопасности (в соответствии со стандартом ISO / IEC 15408) на основе CASE-подхода с использованием формальных нотаций. На основе произведённого анализа, наиболее распространенных нотации для представления обоснований, был осуществлен выбор нотации IT-Trust для формализации требований гарантий безопасности. В ходе работы была разработана методика построения Assurance Case в нотации IT-Trust на основе класса "анализ уязвимости".

Ключевые слова: *безопасность информационных технологий, единые критерии, обоснование безопасности, обоснование гарантии, нотация Тулмина, ASCAD, нотации IT-Trust.*

Введение

Постановка проблемы и анализ литературы. Неблагоприятная обстановка в мире, недобросовестная конкуренция, заставляют общество повернуться лицом к проблеме обеспечения безопасности информационных технологий (ИТ). Главная цель ИТ-безопасности заключается в обеспечении возможности любой организации решать свои функциональные задачи путем построения ИТ-систем, которые исключают или минимизируют ИТ-риски организации, ее партнеров и потребителей. Соответственно задача обеспечения безопасного функционирования информационно-управляющих систем требует совершенствования методов оценки реального уровня безопасности и соответствия требованиям нормативной базы и спецификации [1 – 5].

Следует также отметить, что на сегодняшний день в мире изменилась сама концепция обеспечения ИТ-безопасности. Она учитывает теоретические, технические и социологические изменения, произошедшие в области ИТ. Осуществлен принципиальный переход от ориентации на построение системы защиты информации на объекте к построению системы обеспечения безопасности информации объекта [1].

Как показал анализ, по уровню систематизации, полноте и возможностям детализации требований, универсальности и гибкости в применении наиболее совершенный из существующих в настоящее время стандартов является международный стандарт ISO / IEC 15408-99 ("Общие критерии"(ОК) или Единые критерии) [1 – 4]. Базовыми документами, которые легли в основу Общих критериев, являются: Оранжевая книга (TCSEC) 1985 г., Европейские критерии (ITSEC) 1991 г., Канадские критерии 1993 г., Федеральные критерии США 1993 г.

Опыт использования ОК в мире и опыт, полученный при апробации в Украине, говорит о том, что применение методологии ОК способствует существенному повышению качества оценки и разработки продуктов и систем ИТ [4]. Также следует отметить, что новая идеология построения систем безопасности информации уже реально воплотилась в новую технологию проектирования систем обеспечения ИТ-безопасности.

Однако, существующие методы оценки и обоснования ИТ-безопасности являются не универсальными, недостаточно формализованными и практически не автоматизированными, что показывает потребность в совершенствовании моделей и методов оценки, в разработке более универсальных и гибких методик и инструментальных средств оценки. Одним из важнейших направлений является использование SafetyCase методологии и построение обоснований безопасности с использованием формальных нотаций [4].

Значительный вклад в развитие этой методологии внесли работы западных ученых П. Бишопа, Р. Блумфилда, Т. Келли, Р. Хокинса, Я. Горски и др. [5 – 11].

Целью и задачей данного исследования является формализация требований гарантий безопасности (в соответствии со стандартом ISO / IEC 15408) на основе case-подхода.

Основной материал

Логика построения системы информационной безопасности обусловлена концепцией и моделью ИТ-безопасности, введенной в стандарте ISO/IEC 15408. Заложенная в него технология проектирова-

ния систем обеспечения ИТ-безопасности выделяет три линии или позиции убеждения:

– первая – технология проектирования основана на разработке профиля защиты (ПЗ) и проекта безопасности (ПБ) что является основой технологии проектирования системы обеспечения ИТ-безопасности;

– вторая – каждый этап уже сейчас имеет нормативную поддержку, в виде принятых или разрабатываемых международных стандартов, а также нормативных документов национальных органов по стандартизации государств, поддерживающих ОК;

– третья – каждый этап имеет достаточно проработанную инструментальную поддержку, что обеспечивает эффективное решение задач ИБ на программно-техническом уровне.

На практике требования ИТ-безопасности конкретизируются в функциях безопасности, а затем реализуются через множество механизмов безопасности в конкретный программно-технический объект. В терминах ОК таковым является объект оценки (ОО) (TOE-Target of Evaluation) – ИТ-продукт или ИТ-система, а также связанная с ними эксплуатационная, техническая, пользовательская и иная документация, являющиеся объектом проверки и оценки [12]. Основными документами, характеризующими ТОЕ с точки зрения обеспечения ИТ-безопасности являются профиль защиты и проект безопасности.

Профиль защиты является нормативным документом, который регламентирует все аспекты ИТ-безопасности в виде совокупности требований ИТ-безопасности, предъявляемых к функциям безопасности и, следовательно, к механизмам безопасности и средствам защиты.

Международный стандарт ISO / IEC 15408-99 предусматривает создание специальной электронной картотеки пакетов требований безопасности, ПЗ и ПБ. Данная картотека уже доступна разработчикам, что позволяет минимизировать затраты на разработку новых ПЗ, учесть опыт предыдущих разработок, обеспечить реальную взаимосвязь и совместимость разрабатываемых продуктов, а также повысить взаимопонимание разработчиков систем ИТ-безопасности различных государств.

Требования ИТ-безопасности являются уточнением, конкретизацией и практическим отображением задач защиты и включают в себя три компоненты:

– функциональные требования (ФТ) безопасности;

– требования адекватности;

– требования безопасности к среде эксплуатации.

В ходе разработки ПЗ осуществляется выбор требований безопасности, специфичных для конкретной среды. Выбор осуществляется на основе оценки эффективности реализации данных требований для решения задачи противодействия угрозам безопасности. ФТ определяют свойства безопасности и характеризуют функции безопасности ТОЕ, которые являются типичными для поддержки ИТ-безопасности. При этом ОК отличаются особенно тщательной проработкой ФТ.

При разработке ПЗ учитываются связи, как между различными ФТ, так и между ФТ и требованиями адекватности.

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 [13]:

– составить точный ряд утверждений относительно системы;

– определить подтверждающие доказательства;

– предоставить ряд аргументов в пользу безопасности, которые связывают между собой утверждения с доказательствами;

– детализация, основанная на анализе и оценке;

– разъяснить предположения и суждения, лежащие в основе аргументов;

– предоставить различные точки зрения и уровни детализации.

Предлагаемая методология Safety Case представляет собой систему принципов, методов, методик и программных средств, CASE нотаций, 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.

Прежде чем использовать различные методы оценки важно формализовать сам процесс предстоящей оценки. Это можно сделать с помощью одной из формальных нотаций, таких как UML, Ascad, GSN Trust-IT [5-16]. Выбор формальной нотации зависит от типа системы, сложности её структуры. Формализация процесса оценки позволяет структурировать необходимые действия, определить оптимальный подход к оценке и эффективно выбрать наиболее подходящие методы оценки.

При выборе методов оценки предпочтение следует отдавать тем методам, которые имеют инструментальную поддержку. Примерами таких методов можно назвать методы статического анализа, методы автоматического тестирования и другие. Такие методы работают преимущественно с формальными представлениями данных, позволяют частично автоматизировать процесс оценки и предоставляют потенциальную возможность включения их в новые Safety Case ядра для дальнейшего использования в других системах. Это позволит постоянно пополнять коллекцию ядер, а также унифицировать и упростить процесс оценки различных систем в будущем [4]. При оценке проектов и выборе соответствующих методов необходимо придерживаться разработанных стандартов в данной области.

Модель аргументации Тулмина. Система обозначений Тулмина [11] описывает схему структуру типового аргумента. Аргумент считается правильным, если он является обоснованным и все данные или предположения, на которые он опирается, являются истинными.

Нотация ASCAD была разработана, как часть методологии обоснования безопасности Аделарда. Ее основной идеей для представления аргументной структуры является мотив «утверждения-аргументы-доказательства». Выбор аргумента будет зависеть от имеющихся доказательств и типа утверждения. Например, утверждения относительно надежности обычно обосновывают статистическими аргументами, в то время как другие утверждения могут опираться на более качественные аргументы, такие как соблюдение норм и правил [7, 13].

GSN или нотация структурирования целей – это графическая аргументативная система обозначений, разработанная в Йоркском Университете [13, 15]. Аргументы, задокументированные с помощью GSN нотации, могут помочь предоставить гарантию для критических свойств систем, услуг и организаций.

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 [16], в ее основание положена система обозначения Тулмина.

В данном подходе вместо понятия обоснования безопасности используется понятие обоснование доверия. Обоснование доверия (ОД) – 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 [8]. 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. Методология Trust-IT, имеет инструментальную поддержку в виде приложения Trust-IT, созданным для разработки ОД и их применения в различных ситуациях.

Инфраструктура Trust-IT состоит из трех компонентов:

– прикладной компонент – объясняет возможные варианты использования ОД;

– методологический компонент – объясняет, как разработать и вести обоснования достоверности, определяет язык разработки ОД, 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 показана на рис. 1 [8, 16].

Рис. 1. Структура модели аргумента Trust-IT

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

Аргументная стратегия – 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.

Контраргументная стратегия – основная идея, на которой основывается опровержение обоснованного утверждения. Ее можно считать аргументной стратегией для отрицания заключения. Утверждение может иметь большое количество контраргументных стратегий.

Обоснование – отношение между данными и полученным выводом. Оно объясняет, почему при заданных обстоятельствах необходимо или надлежит сделать определенный вывод, если установленные данные или предположения действительно имеют место быть.

Предположение – исходное допущение без дальнейшего обоснования. Это свойство, не зависимое от того, кто предоставляет ОД.

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 ОД источниках.

Указатель – связь с внешним по отношению к данному обоснованию доверия миром. Она 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 ОД.

Информация – дополнительная информация, не являющаяся частью аргумента. Она содержит пояснительную информацию, которая может помочь понять значение ОД, или помогает организовать структуру ОД.

Ссылки – внутренний указатель, направленный от одного элемента ОД к другому и показывающий связь между элементами. Используя ссылки, можно избежать древовидной структуры ОД и сделать ее в виде направленного ациклического графа. Данная структура может расти в глубину. Следовательно, ОД могут быть разработаны путем предоставления более детальных аргументов для утверждения и некоторых обоснований, до тех пор, пока они не будут полностью подтверждены. Благодаря тому, что аргументная модель может быть применена для представления как формального вывода, так и неформальной аргументации. Она предоставляет способы представления аргументов на основе выскоформализованного анализа, равно как и неопределенных доказательств и индуктивных выводов, которые часто встречаются в реальных ситуациях [5, 8, 16].

В данной статье представлена методика построения Assurance Case в нотации Trust-IT на основе ISO\IEC 15408.

Класс AVA: Обзор уязвимостей. Класс AVA связан с наличием пригодных для использования скрытых каналов и с возможностью неправильного применения или конфигурирования ОО, а также с возможностью преодоления вероятностных или перестановочных механизмов безопасности и использованием уязвимостей, вносимых при разработке или эксплуатации ОО. На рис. 2 показаны семейства этого класса и иерархия компонентов в семействах на основе ISO\IEC 15408 [12].

Анализ скрытых каналов (AVA_CCA) выполняют с целью сделать заключение о существовании и потенциальной пропускной способности (ПС) непредусмотренных каналов передачи сигналов (т.е. неразрешенных информационных потоков), которые могут быть использованы. Требования доверия связаны с угрозой существования непредусмотренных и пригодных для использования путей передачи сигналов, которые могут быть применены для нарушения политики функции безопасности (ПФБ). Компоненты ранжированы по повышению строгости анализа скрытых каналов. Оценка ПС канала основана на технических расчетах, а также на фактических результатах выполнения тестов. Примеры предположений, на которых основан AVA_CCA, могут включать в себя быстродействие процессора, системную или сетевую конфигурацию, размер памяти, размер кэш-памяти.

Выборочное подтверждение правильности анализа скрытых каналов путем тестирования дает оценщику возможность верифицировать любые аспекты анализа (такие, как идентификация, оценка ПС, удаление, мониторинг, сценарии применения). Семейство AVA_MSU позволяет установить, может ли ОО быть конфигурирован или использован опасным образом так, чтобы администратор или пользователь ОО считал бы его безопасным.

Целями AVA_MSU являются:

– минимизация вероятности конфигурирования или установки ОО опасным образом, исключающим возможность обнаружения пользователем или администратором;

– минимизация риска ошибок, обусловленных человеческим фактором или иными причинами, в операциях, которые могут блокировать, отключить или помешать активизировать функции безопасности, приводя к необнаруженному опасному состоянию.

Компоненты ранжированы по возрастанию числа свидетельств, представляемых разработчиком, и повышению строгости анализа.

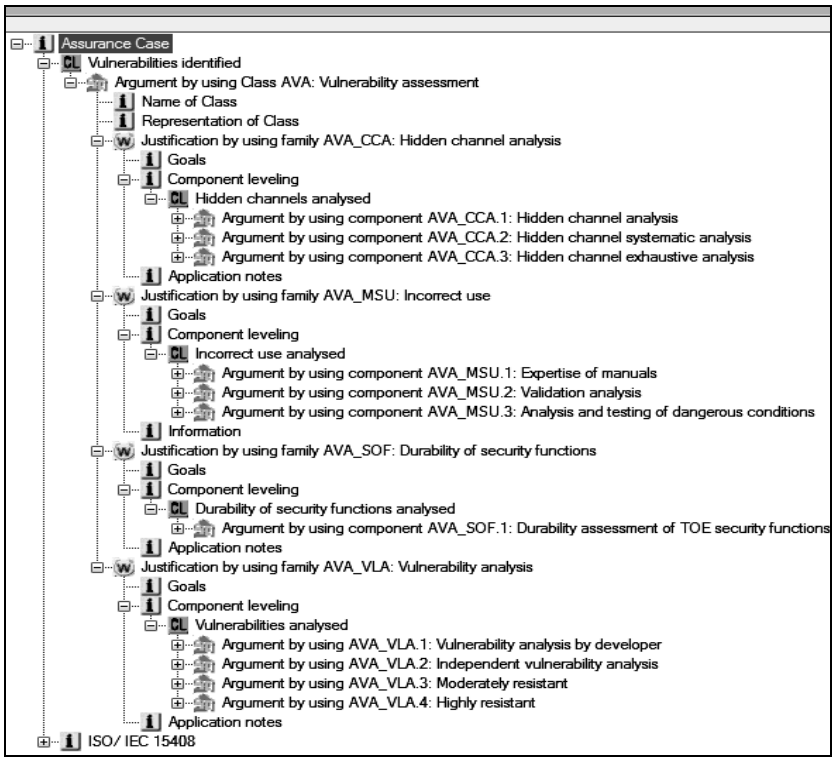

Рис. 2. Декомпозиция класса "Оценка уязвимостей" на основе ISO\IEC 15408

Семейство класса AVA_SOF. Даже если функцию безопасности ОО нельзя обойти, отключить или исказить, в некоторых случаях все же существует возможность ее преодоления из-за уязвимости в концепции реализующих ее базовых механизмов безопасности. Для этих функций квалификация режима безопасности может быть проведена с использованием результатов количественного или статистического анализа режима безопасности указанных механизмов, а также усилий, требуемых для их преодоления. Квалификацию осуществляют в виде утверждения о стойкости функции безопасности ОО.

Разработчик выполняет анализ уязвимостей (AVA_VLA), чтобы установить присутствие явных уязвимостей безопасности и подтвердить, что они не могут быть использованы в предполагаемой среде ОО. Оценщику следует предусмотреть дополнительные тесты для уязвимостей, выявленных при выполнении других частей оценки и потенциально пригодных для использования.

Использование такого подхода обеспечивает гарантии системы, которые определяется как оправданная уверенность в том, что система функционирует, как требуется и свободна от эксплуатационных уязвимостей (ЭУ), намеренно или непреднамеренно созданных или добавленных как часть системы в любое время жизненного цикла. Обеспечить отсутствия ЭУ обычно на практике не достижимо, поэтому программы должны выполнять контроль факторов риска, чтобы уменьшить вероятность и воздействие уязвимостей до приемлемых уровней. 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 ЭУ.

Обоснования гарантии системы целесообразны в ситуациях, когда необходим рациональный базис уверенности в продукте. Целью обоснования гарантии является предоставление заинтересованным лицам убедительного обоснования того, что особо важные требования по обеспечению надежности соблюдаются в ожидаемых системных условиях. В свою очередь, 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.

В системном проектировании разработка и ведение обоснования гарантии должны быть выполнены как часть определения требований заинтересованных лиц, анализа требований, архитектурного анализа.

Вывод

Обеспечения безопасного функционирования ИТ-систем требует совершенствования методов оценки реального уровня безопасности и соответствия требованиям нормативной базы и специфика-

ции. Необходим переход к новой концепции обеспечения ИБ. Как показал анализ, наиболее совершенный из существующих в настоящее время стандартов является международный стандарт ISO / IEC 15408-99. При этом для совершенствования методов, с помощью которых производится оценка и строятся обоснования безопасности было определенно использование SafetyCase методологии и построение обоснований безопасности с использованием формальных нотаций.

На основе произведённого анализа было обосновано выбор нотации IT-Trust для формализации требований гарантий безопасности. В ходе работы была разработана методика построения Assurance Case в нотации IT-Trust на основе класса "анализ уязвимости".

В дальнейшей 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. Перспективы применения международного стандарта ISO/IEC 15408 в Украине / М.Ф. Бондаренко, Л.В. Скрыпик, И.Д. Горбенко, А.В. Потий // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – 2001. – №3. – С. 7-26.

2. Зайцев О.Е. Формальное моделирование «общих критериев» как инструмент внедрения и продвижения стандарта ГОСТ Р ИСО/МЭК 15408 / О.Е. Зайцев, А.В. Любимов // Научно-технический вестник Информационные технологии СПб: Информационных технологий, механики и оптики. – 2007. – № 45. – С. 96-104.

3. Кобзарь М. Методология оценки безопасности информационных технологий по общим критериям / М. Кобзарь, А. Сидак. – JetInfo, № 6 (133), 2004. – С. 2-16.

4. ISO/IEC 15408:2000 – Information technology – Security techniques – Evaluation criteria for IT secu-rity.

5. Неткачёва Е.И. Доказательство и обеспечение безопасности с использованием формальных нотаций / Е.И. Неткачёва, В.С. Харченко // Системи озброєння і військова техніка. – 2011. – № 3. – С. 89-97.

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

7. Bloomfield R.E. 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.

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

10. 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.

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

12. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий Руководящий документ. № 187 Гостехкомиссии России. – М.: ГТК РФ, 2002.

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

14. Assurance and Safety Case Environment (ASCE) Help Manual, version 4.1. – 2011.

15. Wilson, S., Kirkham, P. Safety Argument Manager (SAM) User ManuaL // University of York, York/ December 1995.

16. Cyra A Method of Trust Case Templates to Support Standards Conformity Achievement and Assessment / L. Cyra, 2008.

Поступила в редколлегию 20.10.2015

Рецензент: д-р техн. наук, проф. И.В. Рубан, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ФОРМАЛІЗАЦІЯ ВИМОГ ГАРАНТІЙ БЕЗПЕКИ (У ВІДПОВІДНОСТІ ЗІ СТАНДАРТОМ ISO / IEC 15408) НА ОСНОВІ CASE-ПІДХОДУ

І.В. Косенко, О.А. Усачова, М.Р. Стадніченко

У статті описано підхід до побудови інфраструктури використання програмних стандартів. Розглянуто сучасні підходи до формалізації вимог гарантій безпеки (у відповідності зі стандартом ISO / IEC 15408) на основі CASE-підходу з використанням формальних нотацій. На основі зробленого аналізу, найбільш поширених нотації для подання обґрунтувань, був здійснений вибір нотації IT-Безпеки для формалізації вимог гарантій безпеки. В ході роботи була розроблена методика побудови Assurance Case нотації IT-Безпеки на основі класу "аналіз вразливості ".

Ключові слова: *безпека інформаційних технологій, єдині критерії, обґрунтування безпеки, обґрунтування гарантії, нотація Тулміна, ASCAD, нотація IT Trust.*

FORMALIZATION OF THE REQUIREMENTS OF SECURITY GUARANTEES (IN ACCORDANCE WITH ISO / IEC 15408) BASED ON CASE-APPROACH

I.V. Kosenko, O.A. Usachova, M.R. Stadnichenko

The article describes an approach to the construction of infrastructure, use of software standards. Modern approaches to the formalization of the requirements of security guarantees (in accordance with ISO / IEC 15408) based on CASE-approach using formal notations. On the basis of the performed analysis, the most common notation to represent studies, a selection has been made notation of IT Trust to formalize the requirements of security guarantees. The work was developed a method of constructing the Assurance Case notation in the IT Trust on the basis of "vulnerability analysis".

Keywords: *information technology security, common criteria, safety justification, the justification of warranties, notation Toulmin, ASCAD, notation IT Trust.*