МЕТОДЫ И МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 629.735

КЛАССИФИКАЦИЯ МЕТОДОВ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ К БЕЗОПАСНОСТИ ПРОДУКТОВ И СИСТЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

А.В. ПОТИЙ, Д.С. КОМИН, Ю.Н. КОЗЛОВ

Рассмотрены вопросы использования терминов «доверие» и «гарантии» в области оценки безопасности ИТ, как аутентичные английскому термину assurance, даны их определения, контекст и область использования. Приводится классификация методов обеспечения доверия к безопасности продуктов и систем ИТ.

Ключевые слова: доверие, гарантии безопасности, единые критерии.

ВВЕДЕНИЕ

Неотъемлемой частью современных систем и продуктов информационных технологий (ИТ) является комплекс мер по обеспечению безопасности информации, которая хранится, циркулирует или обрабатывается в этих системах (продуктах), особенно – если это информация с ограниченным доступом. Очевидно, что безошибочное, устойчивое и безопасное функционирование систем ИТ практически невозможно осуществить в течение всех стадий ее жизненного цикла вследствие сбоев, ошибок оператора, отказов оборудования, неудовлетворительной организации процесса разработки, недооценки угроз и т.д. Из этого следует, что ошибки, уязвимости и риски будут существовать всегда и изменяться на всех стадиях жизненного цикла системы ИТ. Следовательно, ошибками, уязвимостями и рисками надо управлять в пределах допустимых параметров, т.е., используя технические и организационные меры, необходимо обеспечить приемлемый (в конкретных условиях эксплуатации) уровень доверия (assurance) к системе ИТ. Приемлемое доверие означает удовлетворение системы ИТ специальным заранее определенным требованиям, которые определяются исходя из целей и требований безопасности. Доверие не обеспечивает предоставление объекту каких-либо дополнительных мер безопасности или услуг, а способствует снижению рисков, поскольку уменьшает неопределенность, связанную с уязвимостями системы/объекта ИТ. Существуют различные методы обеспечения доверия, использование которых зависит от объекта оценки, целей и политики безопасности и ряда других факторов. В данной статье на основе анализа существующих методов доверия проведена их классификация. Также рассмотрены вопросы терминологии в отношении термина *assurance*, поскольку в зависимости от контекста использования оно может иметь различный перевод (доверие, гарантии) и различное значение.

1. ASSURANCE – ДОВЕРИЕ ИЛИ ГАРАНТИИ?

Термин *assurance* в среде безопасности информационных технологий используется для описания мер по оценке уязвимостей и остаточных рисков оцениваемого объекта. Забегая вперед, можно сказать, что *assurance* – это современный подход по оценке доверия к безопасности продуктов и систем информационных технологий.

В среде специалистов по информационной безопасности существуют разногласия относительно перевода данного термина на украинский и русский языки. Одни специалисты при переводе с английского используют термин *гарантии*, в то время как другие – термин *доверие*. Ранее этот вопрос исследовался в работах [1, 2], однако при переводе данного термина необходимо учитывать контекст его использования.

Современное понимание подходов оценки информационной безопасности тесно связано с использованием неформальных методов оценивания, и, как следствие, с получением качественных результатов их применения. Вследствие этого значительное место в принятии решений по оценке и понимании результатов такого оценивания потребителем имеют субъективные и психологические факторы. В [1] исследовалось толкование термина *доверие* различными словарями. Например, доверие – уверенность в чьей-нибудь добросовестности, искренности, в правильности чего-нибудь; психическое состояние, в силу которого мы полагаемся на какое-либо мнение, кажущееся нам авторитетным, и потому отказываемся от самостоятельного исследования вопроса, могущего быть нами исследованным и др. Поэтому перевод термина *assurance* как доверие является оправданным при характеристике общей системы безопасности ИТ в целом, независимо от объекта оценивания (продукт или система ИТ, услуга обеспечения безопасности, процесс, персонал, организация и др.).

Из [3, 4] следует понимать, что доверие является такой характеристикой, которая способствует снижению риска, поскольку уменьшает неопределенность, связанную с уязвимостями объекта, таким образом, уменьшая его потенциальную уязвимость и приводя к снижению общего риска, связанного с объектом.

Таким образом, *доверие* – состояние субъекта, вовлеченного в систему создания и использования продуктов и систем ИТ (разработчик, продавец, оценщик, потребитель), характеризующее меру его уверенности в том, что оцениваемый объект соответствует своим целям безопасности. А понятие *обеспечения доверия* следует понимать как совокупность процессов (мероприятий, действий, процедур), направленных на формирование у заинтересованных субъектов доверия к безопасности продуктов и систем ИТ.

С другой стороны термин *assurance* используется в международном стандарте ISO/IEC 15408 [5, 6] (Критерии оценки безопасности информационных технологий) в качестве *системы требований*, которые характеризуют степень корректности реализации функциональных услуг безопасности оцениваемого объекта. В национальном стандарте НД ТЗИ 2.5-004-99 [7] такие требования именуются *требованиями гарантий*, в то время как в ГОСТ Р ИСО/МЭК 15408 [8] (национальный стандарт Российской федерации) *требованиями доверия*. В [2] проанализированы толкования слов доверие и гарантии на предмет возможности их использования в контексте критериев оценки безопасности ИТ. Сделан вывод, что термин *гарантии*, в данном контексте, является более подходящий по смыслу, значению и адекватности английскому термину *assurance*.

Таким образом, в терминологии информационной безопасности можно выделить два толкования английского термина *assurance*. С одной стороны это *гарантии* – набор требований, характеризующий средства, способы и условия обязательные (или рекомендованные) к выполнению в течение всего жизненного цикла ИТ-продукта для обеспечения корректной реализации функциональных услуг безопасности, противостояния угрозам безопасности и обеспечения требуемого уровня защищенности ИТ-продукта [1]; а, с другой стороны, *доверие* – мера уверенности в том, что оцениваемый объект соответствует своим целям безопасности, и связанное с ним понятие *обеспечения доверия* – совокупность процессов, направленных на формирование у заинтересованных субъектов доверия к безопасности продуктов и систем ИТ [3, 4]. При этом *оценка объекта на соответствие требованиям гарантий является одним из методов обеспечения доверия к безопасности продуктов и систем ИТ*.

2. КЛАССИФИКАЦИЯ МЕТОДОВ ОБЕСПЕЧЕНИЯ ДОВЕРИЯ

Существует большое количество методов обеспечения доверия. Выбор необходимого метода обеспечения доверия должен основываться на изучении политики безопасности организации, бизнес требований и вида оцениваемого объекта. Также, немаловажным фактором выбора метода обеспечения доверия является наличие имеющихся ресурсов (временных, кадровых, финансовых и др.). Поэтому для выбора и применения какого-либо метода обеспечения доверия правообладателям могут потребоваться рекомендации специалистов.

Анализ методов доверия позволил их классифицировать:

1) по объекту оценивания:

– оценивание продукта (системы) ИТ;

– оценивание процессов (разработки, создания, функционирования);

– оценивание внешних факторов (среда, организация, персонал и др.);

– комбинированные (уровень 1 ... уровень 7);

2) по региону использования:

– региональные (национальные);

– международные;

3) по юридической силе:

– национальные;

– «де-факто»;

4) по уровню строгости:

– формальные;

– неформальные;

5) по охвату стадий жизненного цикла:

– проектирование/разработка;

– интеграция;

– ввод в эксплуатацию;

– эксплуатация;

– комбинированные;

6) по типу доверия:

– доверие к корректности;

– доверие к эффективности.

Высокоуровневая классификация методов обеспечения доверия выделяет основные три направления: оценивание продукта, оценивание процесса и оценивания внешних факторов. При оценке продукта проверяется непосредственно сам объект и связанная с ним проектная документация по безопасности, независимо от процессов разработки. Наиболее значимым стандартами, регламентирующими метод обеспечения доверия к продуктам, является международный стандарт ISO/IEC 15408 [5] и национальный стандарт НД ТЗІ 2.5-004-99 [7], и связанные с ними работы, в которых представлен метод оценки гарантий информационной безопасности [1, 9, 10]. Оценка процессов включает в себя проверку организационных процессов используемых для производства и эксплуатации объекта в течение его жизненного цикла. Основные из многочисленных методов обеспечения доверия к процессам закреплены в стандартах ISO/IEC 21827 (проектирование безопасности работы систем – модель зрелости) и ISO/IEC 15504 (оценка программного процесса) [11–13]. Оценка внешних факторов включает в себя проверку влияния

условий окружающей среды, вносящих вклад в качество процессов производства и функционирования. К таким факторам относятся персонал и физическая среда. К методам обеспечения доверия к внешним факторам можно отнести ISO 9000 (менеджмент качества). Также актуальным и перспективным направлением в развитие методов обеспечения доверия к внешним факторам, и в частности к персоналу, является разработка методов обеспечения и оценки культуры информационной безопасности [14, 15]. Существуют также комбинированные методы обеспечения доверия, которые охватывают как все объекты оценивания (оценивание продукта, оценивание процесса и оценивания внешних факторов), так и их часть. Классификация методов обеспечения доверия по уровню охвата объектов оценивания представлена в табл. 1:

Таблица 1

Уровни охвата объектов оценки методами обеспечения доверия

Уровень	Доверие к продукту	Доверие к процессу	Доверие к внешним факторам
1	+		
2		+	
3			+
4	+	+	
5	+		+
6		+	+
7	+	+	+

Методы обеспечения доверия к безопасности могут быть закреплены как в национальных (действующих на территории одного государства или региона), так и международных стандартах (как правило, изданных под эгидой Международной организации по стандартизации (ISO)). Примерами национальных стандартов являются нормативные документы НД ТЗІ 2.5-004-99 и НД ТЗІ 2.7-010-09, которые имеют юридическую силу только на территории Украины. К международным стандартам можно отнести ISO/IEC 15408, ISO/IEC 15288 (процессы жизненного цикла системы), ISO/IEC 13335 (руководство по управлению безопасностью ИТ) и др.

Методы обеспечения доверия включают в себя как официальные национальные и международные стандарты, так и стандарты «де-факто» и другие общепринятые методы. Примером стандарта «де-факто» является метод оценки SSE-CMM (SSAM), который является детально документированным методом доверия, однако не является ни национальным, ни международным стандартом. Другим примером стандарта «де-факто» является метод TPEP (надежный процесс оценивания продукта), который, несмотря на распространенность и успешное использование в некоторых государственных учреждениях, также не является стандартом.

По уровню строгости научные методы принято классифицировать как формальные, полуформальные и неформальные. К неформальным методам относятся те, выводы и заключения по которым производятся на основании данных (значений), выраженных словами, словосочетаниями или предложениями (лингвистическими термами) и которые не могут получить количественной оценки. Получение количественных оценок при оценке доверия к безопасности является сложной задачей, ввиду чего подавляющее большинство стандартов, описывающих методы обеспечения доверия, можно отнести к неформальным. Для формализации неформальных методов можно использовать подход, который лежит в основе метода оценки гарантий информационной безопасности [1, 9, 10] и использует математический аппарат лингвистических переменных и нечеткого логического вывода. Другая классификация строгости доверия предложена в ГОСТ Р 54583-2011 [3, 4], суть которой отображена в табл. 2:

Таблица 2

Строгость доверия и его использование

Уровень строгости	Использование доверия
1	Простая «печать утверждения доверия»
2	Заявления о доверии позитивного уровня
3	Конкретные факты, поддерживающие заявленное доверие
4	Конкретные факты, поддерживающие заявленное доверие, которое можно верифицировать
5	Предоставление доверия общей аудитории, например, совету директоров, и признание этой аудиторией
6	Представление доверия аудитории из специалистов по безопасности и признание этой аудиторией

По охвату стадий жизненного цикла методы обеспечения доверия могут предназначаться как для конкретной стадии, так и для нескольких стадий жизненного цикла (рис. 1). Например, метод обеспечения доверия, предоставляемый стандартом ISO/IEC 15408, охватывает все стадии жизненного цикла оцениваемого объекта (проектирование, разработка, интеграция, ввод в эксплуатацию, эксплуатация); метод SE-CMM (модель технологической зрелости системного проектирования) – охватывает только две стадии: стадию проектирования и стадию интеграции; метод ISO/IEC 17799 (практические правила управления информационной безопасностью) – охватывает только стадию функционирования.

Среди методов обеспечения доверия также различают методы обеспечения доверия к эффективности и доверия к корректности. При обеспечении доверия к корректности дается ссылка на оценку объекта с целью верификации корректности его внедрения в соответствии с

проектом. Напротив, доверие к эффективности относится к способности функций безопасности объекта противостоять осознанным или идентифицированным угрозам. С целью получения общего доверия объект должен быть оценен как на предмет корректности проекта, внедрения и эксплуатации (элемент корректности), так и должен обладать соответствующими функциональными возможностями обеспечения безопасности для противостояния идентифицированным угрозам (элемент эффективности).

ЗАКЛЮЧЕНИЕ

Одно из ключевых мест в области оценки безопасности продуктов и систем ИТ принадлежит английскому термину *assurance*. В зависимости от контекста использования может переводится как *гарантии*, либо *доверие*. Доверие характеризует меру уверенности субъекта в том, что система ИТ соответствует своим целям безопасности, а методы обеспечения доверия являются совокупностью процессов, направленных на формирование у субъектов доверия к безопасности ИТ. Гарантии же являются системой требований, оценка которых позволяет судить о корректности реализации функций безопасности в системе ИТ. Таким образом, оценка объекта на соответствие требованиям гарантий является одним из методов обеспечения доверия к безопасности продуктов и систем ИТ.

Анализ методов обеспечения доверия позволил провести их классификацию. В статье методы обеспечения доверия классифицированы: по объекту оценивания; по региону использования; по уровню строгости; по охвату стадий жизненного цикла; по типу доверия. Классификация позволяет облегчить поиск и выбор необходимого метода доверия в зависимости от условий эксплуатации и целей безопасности системы или продукта ИТ.

Литература

[1] *Потий А.В.* Системно-онтологический анализ предметной области оценивания гарантий информационной безопасности / А.В. Потий, Д.С. Комин // Радіоелектронні і комп'ютерні системи. Науково-технічний журнал. – 2010. – № 5(46). – С. 50–56.

[2] Потий А.В. Оценка гарантий информа¬ционной безопасности на основе функционально-лингвистического подхода / А.В. Потий, Д.С. Комин // Прикладная радиоэлектроника. – 2010. – Том 9. – № 3. – С. 421–435.

[3] ISO/IEC TR 15443-1:2005, Information technology – Security techniques – A framework for IT security assurance – Part 1: Overview and framework.

[4] ГОСТ Р 54581-2011/ISO/IEC TR 15443-1:2005, Информационная технология – Методы и средства обеспечения безопасности – Основы доверия к безопасности – Часть 1: Обзор и основы.

[5] ISO/IEC 15408-1:2005, Informational technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.

[6] ISO/IEC 15408-3:2005, Informational technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirement.

[7] НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22.

[8] ГОСТ Р ИСО/МЭК 15408-1, Информационная технология – Методы и средства обеспечения безопасности – Критерии оценки безопасности информационных технологий – Часть 1: Введение и общая модель.

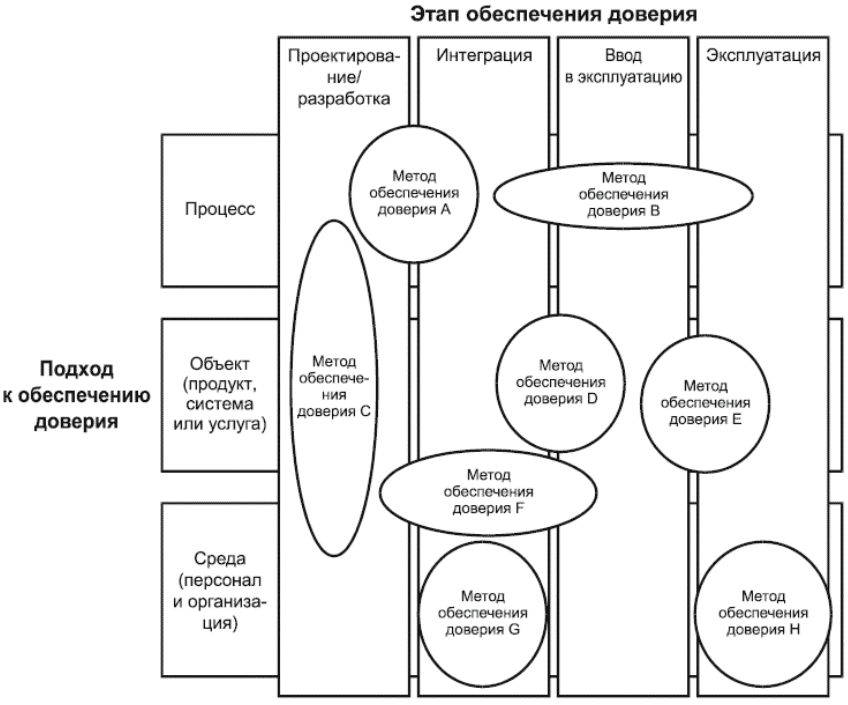

Рис. 1. Охват стадий жизненного цикла методами обеспечения доверия

[9] *Потий А.В.* Формальное описание процесса оценивания гарантий информационной безопасности / А.В. Потий, Д.С. Комин, В.И. Новиков // Системи управління, навігації та зв'язку. – 2011. – № 4 (20). – С. 246–249.

[10] *Потий А.В.* Метод оценивания требований гарантий информационной безопасности / А.В. Потий, Д.С. Комин // VI-я Международная научно-практическая конференция «Наука и социальные проблемы общества: информатизация и информационные технологии». Сборник научных трудов. – Харьков: ХНУРЭ, 2011. – С. 221–222.

[11] *Потій О.В.* Формалізована модель діяльності із захисту інформації / О. В. Потій // Радіоелектронні і комп'ютерні системи. – 2007. – №6 (25). – С. 96–103.

[12] *Потій О.В.* Методичні аспекти оцінки зрілості процесів захисту інформації в умовах невизначеності / О. В. Потій, А.В. Лєншин // Прикладна радіоелектроінка. – 2006. – Том 5, №1. – С. 134-138.

[13] *Потій О.В.* Онтологічі моделі властивостей зрілості процесів захисту інформації / О. В. Потій, // Прикладна радіоелектроінка. – 2009. – Том 8. – С. 112–120.

[14] *Потій О.В.* Властивості діяльності із забезпечення захисту інформації як системної категорії / О.В. Потій, Д.Ю. Пилипенко // Прикладна радіоелектроніка. – 2012. – Том 11. – № 2. – С. 299–303.

[15] *Potiy A.V.* The prerequisites of information security culture development and an approach to complex evaluation of its level / A.V. Potiy, D.Y. Pilipenko, I.N. Rebriy // Радіоелектронні і комп'ютерні системи. – № 5 (57). – 2012. – С. 72–77.

Поступила в редколлегию 12.05.2014

Потий Александр Владимирович, фото и сведения об авторе см. на стр. 260.

Комин Дмитрий Сергеевич, кандидат технических наук, научный сотрудник научного центра Воздушных Сил Харьковского университета Воздушных Сил им. И. Кожедуба. Научные интересы: методы системного анализа процессов защиты информации; методы оценки безопасности объектов информационной деятельности.

Козлов Юрий Николаевич, фото и сведения об авторе см. на стр. 260.

УДК 629.735

Класифікація методів забезпечення довіри щодо безпеки продуктів та систем інформаційних технологій / О.В. Потій, Д.С. Комін, Ю.М. Козлов // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 311–315.

Розглянуто питання використання термінів «довіра» та «гарантії» в області оцінки безпеки ІТ, як аутентичні англійському терміну assurance, надано їх визначення, контекст та область використання. Наводиться класифікація методів забезпечення довіри щодо безпеки продуктів та систем ІТ.

Ключові слова: довіра, гарантії безпеки, єдині критерії оцінки інформаційної безпеки.

Табл.: 2. Іл.: 1. Бібліогр.: 15 найм.

UDK 629.735

Classification of methods of trust assurances to security of IT products and systems / A.V. Potiy, D.S. Komin, Yu.N. Kozlov // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 311–315.

Translation problems of the term «assurances» in the IT security sphere are considered. A classification of security assurances methods to IT systems and products is presented.

Keywords: trust, security assurances, common criteria.

Tab.: 1. Fig.: 1. Ref.: 15 items.