УДК 629.735

**А.В. ПОТИЙ, Д.С. КОМИН**

***Харьковский университет Воздушных Сил им. И. Кожедуба, Украина***

# СИСТЕМНО-ОНТОЛОГИЧЕСКИЙ АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ ОЦЕНИВАНИЯ ГАРАНТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Приводятся результаты онтологического анализа предметной области гарантий информационной безопасности. Дается обоснование применения в технической литературе понятий "требования гарантий" и "требования доверия" в области обеспечения информационной безопасности. Строятся онтологии предметной области понятий "гарантии безопасности", "требования и уровня гарантий", "оценка гарантий безопасности", уточняются термины и определения в данной сфере.*

***Ключевые слова:*** *гарантии безопасности, уровень гарантий, оценивание гарантий, онтологическое моделирование.*

## Введение

Методологической основой современных технологий проектирования защищенных систем информационных технологий (ИТ-систем) и комплексных систем защиты информации (КСЗИ) являются международный стандарт ISO/IEC 15408 [1,2] и национальный нормативный документ НД ТЗИ 2.5-004-09 [3]. Эти документы предполагают выдвижение функциональных требований безопасности и требований гарантий, которые в ходе проектирования подлежат оцениванию на предмет их выполнения. Многолетний опыт применения этих нормативных документов сделали особенно актуальными задачи обеспечения и оценки гарантий безопасности (уровня доверия).

В общей проблеме обеспечения гарантий безопасности основополагающая роль принадлежит научно-теоретическому аспекту. В рамках данного аспекта можно выделить следующие разделы:

- терминология;
- стандартизация в сфере обеспечения гарантий безопасности;
- критерии оценки гарантий безопасности;
- способы определения (выбора) и обоснования требований и уровня гарантий;
- методы оценки уровня гарантий безопасности;
- модели процессов обеспечения гарантий безопасности;
- методы анализа уровня гарантий в ходе эксплуатации КСЗИ.

Терминология является инструментом взаимодействия и необходимым условием единства подходов к решению различных задач обеспечения гарантий. Активно развивается стандартизация в данной сфере, о чем свидетельствует разработка проектов стандартов НД ТЗИ 2.7-010-09 [4], ISO/IEC 18045 [5]. При определении и обосновании требований и уровня гарантий в основном применяются методы системного анализа (эвристические методы, методы экспертной оценка и т.д.).

Оценка уровня гарантий сегодня осуществляется по приближенным методикам, которые носят неформальный характер.

Степень доверия к результатам оценивания (в любой сфере) определяется качеством и количеством усилий и ресурсов, затраченных на его проведение. Уровень оценки характеризуется широтой, т.е. степенью охвата элементов объекта оценивания, глубиной, т.е. детальностью рассматриваемых материалов об объекте оценивания и строгостью, т.е. уровнем формализации применяемых методов оценивания и качеством инструментальных средств оценки [6].

На сегодняшний день можно с уверенностью говорить, что, как на национальном, так и на международном уровне, отсутствует какой-либо цельный научно-методический аппарат оценки гарантий безопасности.

В настоящее время формируются основные принципы и подходы к решению этой задачи, о чем свидетельствует активная работа над проектами международных стандартов [7].

Все выше изложенное говорит о том, что создание формального научно-методического аппарата оценки гарантий безопасности, разработка методов оценки уровня гарантий, которые способны обеспечить строгость оценки и лягут в основу разработки инструментальных средств оценки является актуальной научно-технической задачей в сфере защиты информации.

В данной работе изложены результаты системно-онтологического анализа предметной области оценивания гарантий безопасности, который проводился с целью уточнения основных понятий в данной предметной области.

## 1. Анализ предметной области обеспечения гарантий безопасности

В исторической ретроспективе требований гарантий безопасности были впервые закреплены в международном стандарте ISO/IEC 7498-2 [8]. В данном стандарте вводится общий механизм безопасности доверительная функциональность, под которой понимается совокупность рекомендаций и способов, реализуемых для обеспечения гарантий правильной и надлежащей работы других механизмов безопасности.

Позже, в документу NIST SP 800-30 [9], вводится базовая техническая модель защиты информации в основу которой заложены пять основных целевых задач обеспечения безопасности информации, а именно обеспечение конфиденциальности данных и системной информации, целостности данных и системы, доступности (системы, данных, ресурсов), наблюдаемости и гарантий безопасности. Именно в этом документе нормативно закрепляется понятие гарантий (assurance), под которым понимают обеспечение того, что перечисленные выше задачи будут адекватно удовлетворены. Это основа уверенности в том, что принятые меры защиты как технического, так и организационного характера реализованы корректно. Гарантированность – существенное требование, без которого реализация всех остальных требований безопасности бессмысленна [9].

Окончательно необходимость и обязательность выдвижения и обеспечения требований гарантий были закреплены в международном стандарте ISO/IEC 15408. Согласно [1,2] требования безопасности должны включать функциональные требования безопасности и требования гарантий (доверия).

*Функциональные требования безопасности* определяют требования к функциям ИТ-системы, реализующим их механизмам и средствам защиты, которые непосредственно предназначены для обеспечения безопасности и определяют предусмотренный режим безопасности. К функциональным требованиям относятся, в частности, требования идентификации, аутентификации, аудита безопасности и др.

*Требования гарантий (доверия)* это требования, выполнение которых дает основание для уверенности в том, что ИТ-система обеспечивает достижение поставленных целей безопасности. Требования гарантий (доверия) включают совокупность требований к необходимым действиям разработчика ИТ-системы, к предоставлению соответствующих свидетельств обеспечения требуемого уровня безопасности и к действиям при оценке безопасности ИТ-системы. В их состав входят требования к [2]:

- поддержке жизненного цикла;
- процессу разработки;
- управлению конфигурацией;
- эксплуатационной документации;
- тестированию;
- анализу уязвимостей;
- поставке и вводу в эксплуатацию;
- поддержке доверия к безопасности при эксплуатации.

Тем не менее, до настоящего времени еще в среде специалистов есть определенная несогласованность и как переводить англоязычный термин *assurance*, и что понимать под ним. В различных документах, научной литературе предлагаются и различные переводы и различные определения этого термина. Термин *assurance* переводят и как доверие (российская нормативная база) и как гарантии (украинская нормативная база), и определяют его, например, как основание для уверенности в том, что сущность отвечает своим целям безопасности [1]; основа для уверенности в том, что продукт или система ИТ отвечают целям безопасности [2]; выполнение соответствующих действий или процессов для предоставления уверенности в том, что объект оценки, будет удовлетворять своим целям безопасности [7]; совокупность требований (шкала оценок) для определения меры уверенности, что компьютерная системы корректно реализует политику безопасности [10]; мера уверенности в том, что информационно-коммуникационная система корректно реализует политику безопасности [11].

Авторами был проведен анализ понятий «гарантии» и «доверие», на основе которого сделаны следующие выводы.

Российские специалисты при переводе международного стандарта термин *assurance* перевели как *доверие*. Обосновывают это тем, что использование термина, однокоренного слову «гарантия», для перевода термина *assurance,* неприемлемо ввиду возможности его интерпретации в юридическом смысле [6]. В этом есть определенный смысл, но использование слова «доверие» не менее неподходящее, чем использования слова «гарантии».

Исходя из определений термина *доверие*, которые были рассмотрены авторами, можно сделать вывод, что *доверие* это, прежде всего психологическое состояние субъекта, в силу которого субъект полагается на чужое мнение. По большей части это относится к эмоциональной, т.е. плохо рационализируемой сфере психики. Сам же термин *assurance*

включает в себя больше технический аспект и отображает меры, которые должны быть приняты на всех этапах жизненного цикла ИТ-системы для обеспечения уверенности в выполнении предъявляемых функциональных требований. Поэтому не совсем верно характеризовать какие-либо меры термином доверие, поскольку термин имеет психологическое весьма субъективное значение.

В какой-то степени можно говорить о доверии к предпринимаемым контрмерам, но о том, что доверие является характеристикой этих контрмер – говорить сложно, поскольку доверием можно характеризовать лишь психологическое состояние человека.

В украинской терминологии в области защиты информации [3, 11] предлагается использование термина *гарантии*, и соответствующие ему требования называют требованиями гарантий. С одной стороны нельзя не отрицать, что использование этого термина имеет ограничение из-за возможности его трактовки в юридическом смысле, поскольку ни международные, ни отечественные стандарты не предполагают каких либо юридических обязательств ни разработчика, ни владельца ИТ-системы относительно выполнения этих требований. Однако, анализ определений данного термина в различных сферах деятельности позволяет говорить, что *гарантии* это не только юридические обязательства, но и средства, способы, условия и заверения выполнения чего-либо. Поэтому если не учитывать юридической составляющей данного понятия, то использование данного термина, на наш взгляд, более приемлемо при описании, характеристики и оценке требований безопасности.

Толкование термина *assurance* в английском языке означает намерение вселить уверенность, обещание, залог, поручительство, гарантии, страхование, свободу от сомнений. А антонимом в английском языке данному слову является слово *uncertainty* – неопределенность. Поэтому использование термина *гарантии* более адекватно английскому термину *assurance,* чем *доверие.* Кстати, ни один англо-русский словарь не дает перевода слова *assurance,* как доверие, а переводится как уверение, гарантия, заверение, уверенность, убежденность, страхование.

Таким образом, в данной работе и далее при исследовании предметной области оценки информационной безопасности мы будем использовать термин *гарантии*, как более подходящий по смыслу, значению и адекватности английскому термину *assurance.*

Исходя из всего вышесказанного, можно дать следующее определение:

*Гарантии безопасности* – это средства, способы и условия обязательные (или рекомендованные) к выполнению в течение всего жизненного цикла ИТ-системы для обеспечения корректной реализации функциональных услуг безопасности, противостояния угрозам безопасности и обеспечения требуемого уровня защищенности ИТ-системы.

В основном объектом приложения требования гарантий являются организационные и технологические процессы проектирования, разработки и эксплуатации ИТ-систем, а задача эксперта подтведить выполнение этих требований для формирования уверенности потребителя (или самого же разработчика) в заявленном уровне информационной безопасности.

## 2. Онтологические моделирование предметной области гарантий безопасности

### 2.1. Задача онтологического анализа предметной области

Анализ предметной области представляет особый вид научной деятельности, в результате которого строится интерпретационная модель предметных знаний (в широком смысле). В процессе анализа последние делятся на инвариантные и прагматичные знания, концептуальные составляющие которых представляют онтологические знания предметной области [12]. Новым направлением в области средств и методов системного анализа предметной области является системно-онтологический анализ. Центральной идеей системно-онтологического подхода является разработка онтологической системы (ОнС). Такая система описывается выражением (1) и представляет онтологию предметной области (ПдО), состоящую из онтологии объектов, онтологии процессов и онтологии задач [12]:

$$ОнС = \{О^{ПоО}(О^{О}, О^{П}), О^{З}\} \qquad (1)$$

где $О^{О}$ – онтология множества объектов (понятий, концептов) ПдО, рассматриваемая как иерархическая структура классов, подклассов и элементов классов; $О^{П}$ – онтология множества процессов ПдО, рассматриваемая как иерархическая структура процессов, подпроцессов, действий и операций; $О^{З}$ – онтология совокупности задач, которые могут быть поставлены и решены в ПдО и рассматриваемая как иерархическая структура задач, подзадач, процедур и операторов.

Под онтологией множества понятий понимается кортеж четырех множеств [12]:

$$Оо = <X, R, F, A(D, Rs)>, \qquad (2)$$

где $X = \{x_1, x_2, ..., x_i, ..., x_n\}$, $i = \overline{1,n}$, $n = Card\ X$ – конечное множество концептов (понятий) заданной

предметной области; $R = \{r_1, r_2, ..., r_k, ..., r_m\}$, $R: x_1 \times x_1 \times x_2 \times ... \times x_n$, $k = \overline{1,m}$, $m = Card\ R$ – конечное множество семантически значимых отношений между концептами предметной области; $F = X \times R$ – конечное множество функций интерпретации, заданных на концептах и/или отношениях; $A$ – конечное множество аксиом, которые используются для записи всегда истинных высказываний (определений и ограничений).

Первичный анализ нормативных документов [1 – 5, 7 – 10], научно-технической литературы [6, 11] позволил выделить следующие объекты онтологического моделирования:

- термины-объекты: гарантии, уровень гарантий, критерии гарантий, уверенность, программа оценивания, методика оценивания, объект оценки, безопасность информации, меры обеспечения безопасности, уязвимость, угроза, риск, вердикт, общий вердикт;

- термины-процессы: оценивание, аккредитация, сертификация, действие, шаг, проверка, исследование, верификация.

### 2.2. Онтологические модели предметной области гарантий безопасности

На рис. 1 показан контекст безопасности ИТ-систем согласно международному стандарту ISO/IEC 15408. ИТ-безопасность связана с защитой активов от угроз. Во внимание следует принимать все разновидности угроз, но в сфере безопасности наибольшее внимание уделяется тем из них, которые связаны с действиями человека (умышленные и неумышленные). За сохранность рассматриваемых активов отвечают их владельцы, для которых эти активы имеют ценность. Существующие или предполагаемые нарушители также могут придавать значение этим активам и стремиться использовать их вопреки интересам их владельца.

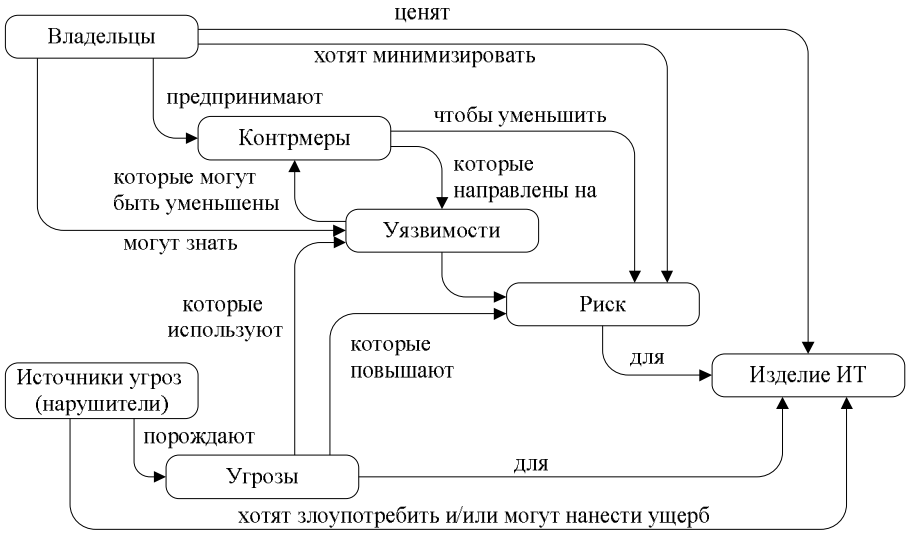


Рис. 1. Взаимосвязь основных понятий в сфере ИТ-безопасности

К специфическим нарушениям безопасности обычно относят (но не обязательно ими ограничиваются): наносящее ущерб раскрытие актива несанкционированным получателем (потеря конфиденциальности), ущерб активу вследствие несанкционированной модификации (потеря целостности) или несанкционированное лишение доступа к активу (потеря доступности).

Владельцы активов будут анализировать возможные угрозы, чтобы решить, какие из них действительно присущи их среде. В результате анализа определяются риски. Анализ может помочь при выборе контрмер для противостояния угрозам и уменьшения рисков до приемлемого уровня.

Контрмеры предпринимают для уменьшения уязвимостей и корректного выполнения политики безопасности. Но и после введения этих контрмер могут сохраняться остаточные риски для активов. Владельцы будут стремиться минимизировать этот риск, задавая дополнительные ограничения.

Прежде чем подвергнуть активы опасности воздействия выявленных угроз, их владельцам необходимо убедиться, что предпринятые контрмеры обеспечат адекватное противостояние этим угрозам. Сами владельцы активов не всегда в состоянии судить обо всех аспектах предпринимаемых контрмер и поэтому могут потребовать их оценку. Результатом такой оценки является заключение о степени доверия контрмерам по уменьшению рисков для защищаемых активов. В этом заключении устанавливается уровень гарантий как результат применения контрмер. Гарантии являются той характеристикой контрмер, которая дает основание для уверенности в их надлежащем действии. Заключение о

результатах оценки может быть использовано владельцем активов при принятии решения о приемлемости риска для активов, создаваемого угрозами. Рис. 2 иллюстрирует эту взаимосвязь. Поскольку за активы несут ответственность их владельцы, то им следует иметь возможность отстаивать принятое решение о приемлемости риска для активов, создаваемого угрозами. Для этого требуется, чтобы результаты оценки были правомерными. Следовательно, оценка должна приводить к объективным и повторяемым результатам, что позволит использовать их в качестве свидетельства.

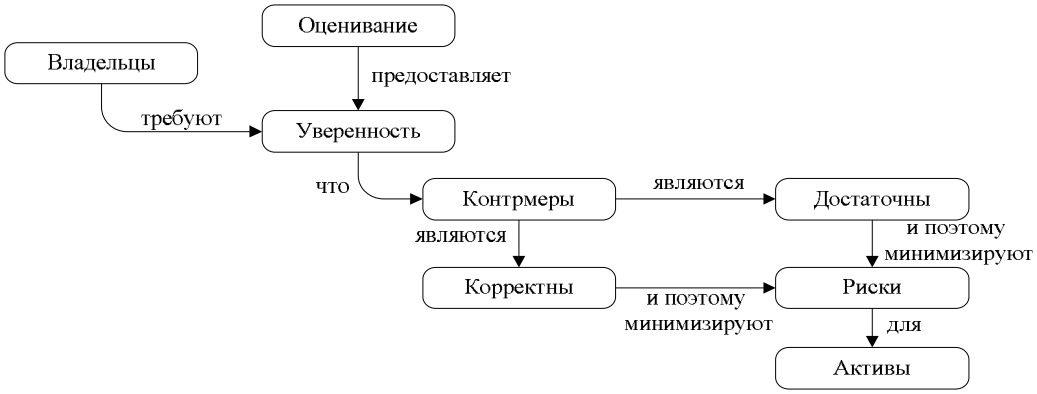


Рис. 2. Понятие оценивания и его значение для владельцев [13]

Онтологическая модель, описывающая предметную область понятий «*уверенность*» и «*гарантии*» представлена на рис. 3. Мерой уверенности в том, что в ИТ-системе обеспечивается требуемый уровень защиты информации, в том, что КСЗИ решает задачи защиты информации является *уровень гарантий (assurance level)*. В свою очередь *уверенность (confidence)* есть вера в то, что ИТ-система (т.е. объект оценки безопасности) будет выполнять задачи защиты соответствующим образом (правда не в одном стандарте пока не определено, что значит соответствующим образом). Уровень гарантий – это совокупность *требований гарантий (assurance requirements)*, выполнение которых характеризует корректность реализации функциональных требований безопасности, способность ИТ-системы противостоять угрозам безопасности и обеспечивать достижение (и сохранения) требуемого уровня защищенности информации в системе. Требования гарантий выдвигаются к *объекту оценки (deliverable)* в качестве которого выступает средство технической защиты информации от несанкционированного доступа (НСД), защищенный от НСД компонент вычислительной системы или комплекс средств защиты (КСЗ) комплексной системы защиты информации (КСЗИ).

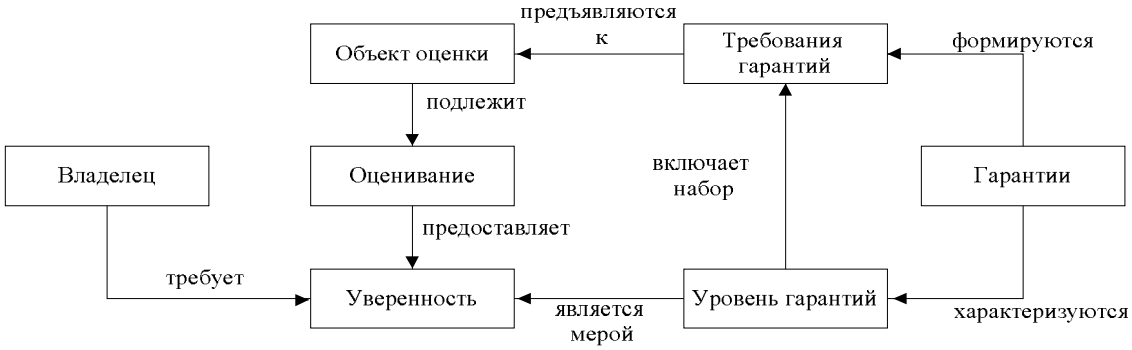


Рис. 3. Онтологическая модель понятий «уверенность» и «гарантии»

В отношении объекта оценки осуществляется процесс *оценивания (evaluation)*, с целью определения выполнения требований гарантий (рис. 4). Процесс оценивания осуществляется на основе *программы* и *методики* оценивания, в рамках сертификации объекта оценки и в соответствии *критериями* оценивания. *Программа оценивания (evaluation program)* – документированная совокупность требований гарантий, которые подвергаются проверке в процессе оценивания объекта оценки. *Методика оценивания (evaluation methodic)* – определенные (установленные) способы проведения оценки требований гарантий. *Сертификация (certification)* – процедура, при которой устанавливается уровень гарантий. Сертификация должна проводиться третьими лицами (независимыми экспертами) с целью пре-

доставления окончательного заключения. В процесс оценивания вовлечены субъекты оценивания – эксперт, орган оценки, владелец ИТ-системы, разработчик ИТ-системы. *Эксперт* – физическое лицо, обладающее соответствующими компетенциями, достаточными для проведения оценивания гарантий безопасности. Учитывая, что есть несколько стадий жизненного цикла объекта оценки, может быть и несколько соответствующих специалистов для оценивания гарантий на том или ином этапе жизненного цикла. *Орган оценки гарантий (assurance authority)* – организация, обладающая соответствующими полномочиями для принятия (утверждения) решений связанных с оцениванием уровня гарантий и выдачи соответствующих документов (сертификатов).

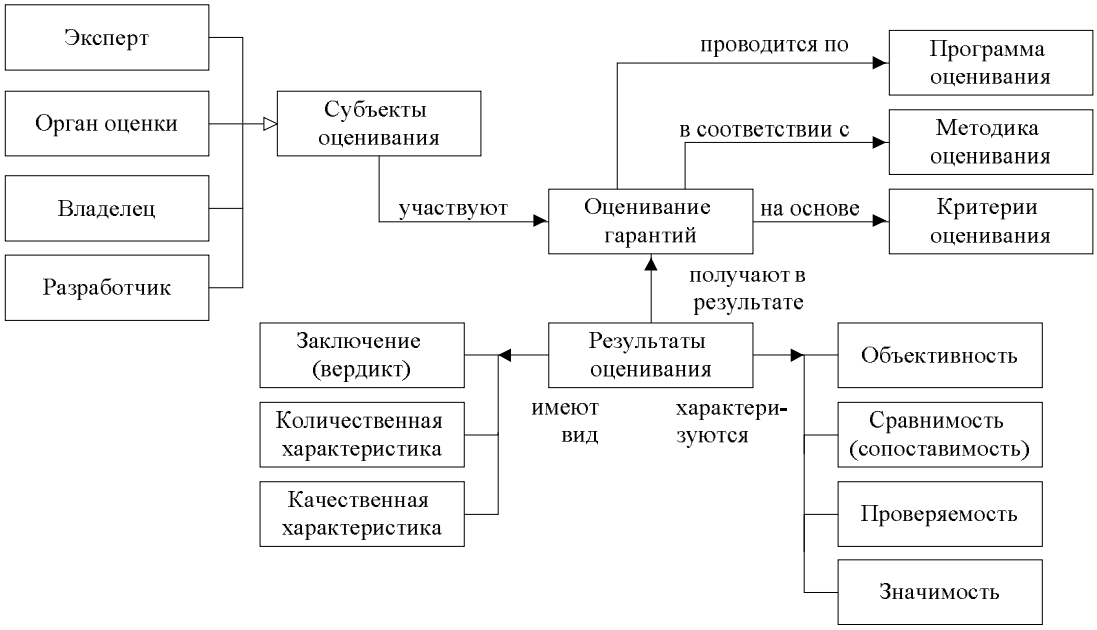


Рис. 4. Онтологическая модель «оценивания гарантий»

*Критерии оценивания (evaluation criteria)* – формальные или неформальные правила, на основе которых принимается решение относительно выполнения требований гарантий.

Выходом процесса оценивания является *результат оценивания гарантий (assurance result)* – задокументированная количественная или качественная характеристика объекта оценивания. К результатам оценивания выдвигаются требования объективности, повторяемости, значимости, проверяемости и сопоставимости (сравнимости).

## Заключение

Обеспечение требований гарантий безопасности является необходимым условием реализации функциональных требований защищенности и обеспечения безопасности информации в целом. На сегодняшний день в нормативных документах определены подходы и рекомендации относительно выбора требований гарантий и обоснования уровня гарантий для объекта оценки. Однако остаются нерешенными как в теоретическом, так и в практическом плане задачи реализации и оценки выполнения требований гарантий. Учитывая, что требования гарантий носят больше неформальный характер, объектом их приложения являются большей частью организационные и технологические процессы (проектирования, разработки, производства) для оценки уровня гарантий необходимо использовать неформальные или формализованные методы системного анализа.

В статье, на основе анализа предметной области гарантий, устранена неоднозначность в переводе и трактовке англоязычного термина "*assurance*". Авторы стоят на позиции, что термин "*гарантии*" является более подходящим, по сравнению с термином "*доверие*".

Рассматривая предметную область "оценивания гарантий", можно выделить следующие нерешенные на сегодняшний день задачи:

– на сегодняшний день практически отсутствуют методы и способы оценки выполнения требований гарантий, что не позволяет обеспечить такую характеристику оценки как строгость;

– отсутствие разработанного научно-методического аппарата оценки гарантий безопасности, как следствие, привело к отсутствию необходимого инструментария, который позволит повысить эффективность работы экспертов по оценке гарантий и обеспечить строгость оценки;

– на сегодняшний день отсутствует системное описание (представление) результатов оценивания гарантий, т.е. не разработаны и не предложены показатели (количественные или качественные), которые могут выступать в качестве объективной основы для принятий решения относительно выполнения требований гарантий.

Нерешенность выше перечисленных задач является основной причиной невозможности обеспечения объективности, сравнимости, проверяемости и значимости результатов оценивания гарантий безопасности.

## Литература


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

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

*3. 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.*

*4. НД ТЗІ 2.7-010-09: Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 24.07.2009 №172.*

*5. ISO/IEC 18045:2005, Informational technology – Security techniques – Methodology for IT security evaluation.*

*6. Трубачев А.П. Оценка безопасности информационных технологий / А.П. Трубачев и др. – М.: СИП РИА, 2001. – 356 с.*

*7. ISO/IEC 15443. Informational technology – Security techniques – A framework for IT security assurance – Part 1: Overview and framework.*

*8. ISO 7498-2:1989. Information processing systems - Open System Interconnection - Basic reference model - Part 2: Security architecture.*

*9. NIST SP 800-30. Stoneburner G. Underlying Technical Models for Information Technology security / G. Stoneburner – NIST, 2002.*

*10. НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.*

*11. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков – К.: ВНV, 2009. – 608 с.*

*12. Палагин А.В. Системно-онтологический анализ предметной области / А.В. Палагин, Н.Г. Петренко, УДК 004.318.*

*13. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model. Version 3.1. Revision 3. Final. CCMB-2009-07-001, July 2009.*


*Поступила в редакцию 28.01.2010*

**Рецензент:** д-р техн. наук, проф., проф. кафедры безопасности информационных технологий В.И. Долгов, Харьковский национальный университет радиоэлектроники, Харьков.

## СИСТЕМНО-ОНТОЛОГІЧНИЙ АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ОЦІНЮВАННЯ ГАРАНТІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

***О.В. Потій, Д.С. Комін***

Наводяться результати онтологічного аналізу предметної області гарантій інформаційної безпеки. Надається обґрунтування застосування у технічній літературі понять вимог гарантій та вимог довіри в області забезпечення інформаційної безпеки. Будуються онтології предметної області понять гарантій безпеки, вимог та рівня гарантій, оцінка гарантій безпеки, уточнюються терміни та визначення у даній сфері.

**Ключові слова:** гарантій безпеки, рівні гарантій, оцінювання гарантій, онтологічне моделювання.

## SYSTEM-ONTOLOGICAL ANALYSIS OF SUBJECT FIELD OF ASSURANCE EVALUATION INFORMATION SECURITY

***A.V. Potij, D.S. Komin***

Give results of the ontological analysis of a subject field of assurance evaluation information security. The application substantiation in the technical literature of concepts of the assurance requirements and trust requirements in the field of maintenance of information security. Construct ontology's of subject field of concepts assurance security, assurance requirements and levels, evaluation of assurance security, terms and definitions in the given sphere are specified.

**Key words:** assurance security, assurance levels, assurance evaluation, ontological modeling.

**Потий Александр Владимирович** – д-р техн. наук, доцент, начальник кафедры радиоэлектронных систем пунктов управления Воздушных Сил Харьковского университета Воздушных Сил им. И. Кожедуба, Харьков, Украина, e-mail: potav@ua.fm.

**Комин Дмитрий Сергеевич** – адъюнкт кафедры радиоэлектронных систем пунктов управления Воздушных Сил Харьковского университета Воздушных Сил им. И. Кожедуба, Харьков, Украина, e-mail: dimakomin@mail.ru.