УДК 621.377

С.А. Смолин, А.С. Корсунский

К ВОПРОСУ О СЕРТИФИКАЦИИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

***Смолин Сергей Анатольевич**, окончил механико-математический факультет Ульяновского государственного университета. Начальник научно-исследовательской лаборатории ФНПЦ ОАО «НПО «Марс». [e-mail: mars@mv.ru].*

***Корсунский Андрей Сергеевич**, кандидат технических наук, окончил факультет радиосвязи Ульяновского филиала Военного университета связи, адъюнктуру Военной академии связи им. С.М. Буденного. Ведущий инженер-программист ФНПЦ ОАО «НПО «Марс». Имеет статьи и изобретения в области радиоэлектронной защиты, безопасности связи и информации. [e-mail: aksspb@mail.ru].*

Аннотация

В статье исследуются вопросы сертификации в области защиты информации. Рассмотрен подход к процедуре сертификации в области защиты информации, дающий возможность обосновать количественные показатели эффективности системы сертификации.

Ключевые слова: сертификация, аттестация, защита информации.

Abstract

The article investigates a issues of certification in the field of information security. It deals with an approach to certification procedure in the field of information security, contributing to reasoning of quantitative factors of certification-system efficiency.

Key words: certification, attestation, information security.

Введение

В настоящее время в области защиты информации имеют место некоторая неоднозначность и противоречивость в вопросе единой терминологии, что связано отчасти с несогласованностью вводимых и действующих законов и нормативных актов, отчасти с целенаправленным манипулированием терминами и понятиями. Поэтому ощущается необходимость в ясных определениях, используемых при оценке соответствия в области защиты информации.

Принятие международных стандартов по управлению качеством (ИСО/МЭК 9000, 9001, 9004), в которых нашли свое отражение новые подходы к оценке и управлению качеством технологических процессов, в том числе процесса защиты информации (обеспечения безопасности информации), также требует согласования терминологии, используемой в них, с другими государственными стандартами.

Разработка отечественной нормативной базы и согласование ее с международными стандартами в области защиты информации требуют внимательного и осторожного подхода, поскольку «источниками вдохновения» для российских разработчиков руководящих документов, как правило, являются документы, разработанные в США; некоторые документы являются аутентичными переводами иностранных стандартов. При этом изменения и дополнения новых редакций этих стандартов в России остаются практически «незамеченными». Необходимо отметить, что и в отечественной нормативной базе также имеют место «внутренние» неточности и несогласованность.

Сертификация в области защиты информации

Известно, что необходимым условием обеспечения требуемого качества продукции, услуг и технологических процессов является выполнение оценки соответствия [11]. Оценка соответствия может принимать следующие формы: государственный контроль (надзор), аккредитация, регистрация, подтверждение соответствия, приемка, ввод в эксплуатацию.

В области защиты информации ситуация несколько осложнена тем, что в соответствии с принятой в нашей стране концепцией защиты информации от несанкционированного доступа, существуют два относительно самостоятельных направления: направление, связанное со средствами вычислительной техники (СВТ), и направление, связанное с автоматизированными системами (АС). Отличие этих направлений заключается в следующем: при рассмотрении вопросов защиты СВТ ограничиваются только

программно-техническими аспектами функционирования системы, а защита АС предполагает рассмотрение организационных мер защиты, вопросов физического доступа, защиты информации от утечки по техническим каналам и т. п. СВТ представляют собой программно-технические средства, разрабатываемые и поставляемые на рынок как элементы, из которых строятся АС. Помимо набора СВТ АС включает в себя обслуживающий персонал и систему организационных мероприятий, обеспечивающих ее функционирование, а также помещения, пользовательскую информацию, бумажную документацию и т. д. Существование двух условно различающихся направлений в защите информации, является причиной отличия используемой в нашей стране терминологии от принятой в других странах.

Поэтому выделяют следующие основные организационно-технические мероприятия по защите информации в общегосударственных информационных и телекоммуникационных системах [1]:

- лицензирование деятельности организаций в области защиты информации;
- аттестация объектов информатизации (ОИ) по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

Проведение аттестации ОИ по требованиям безопасности информации регламентируется рядом нормативных документов [6-8].

Система аттестации ОИ по требованиям безопасности информации является составной частью единой системы сертификации средств защиты информации и аттестации ОИ по требованиям безопасности информации и подлежит государственной регистрации в установленном порядке. Деятельность системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации [5].

Под ОИ, аттестуемыми по требованиям безопасности информации, понимаются АС различного уровня и назначения; системы связи, отображения и размножения документов вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите; помещения, предназначенные для ведения конфиденциальных переговоров.

В состав ОИ входят также технические средства и системы, не обрабатывающие информацию (так называемые, вспомогательные технические средства), размещенные в помещениях, где обрабатывается (циркулирует) информация, содержащая сведения ограниченного распространения, или размещены АС и средства изготовления и размножения документов. При этом, если в одном помещении размещено несколько ОИ, для каждого объекта технические средства, входящие в состав других объектов, будут являться вспомогательными техническими средствами.

Под аттестацией ОИ понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа (Аттестата соответствия) подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Федеральной службой по техническому и экспортному контролю (ФСТЭК). Порядок проведения аттестационных испытаний показан на рисунке 1.

Организационную структуру системы аттестации объектов информатизации образуют:

- Федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации ФСТЭК России;
- органы аттестации ОИ по требованиям безопасности информации;
- испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;
- заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).

Порядок проведения аттестации ОИ по требованиям безопасности информации включает следующие действия:

- подачу и рассмотрение заявки на аттестацию;
- предварительное ознакомление с аттестуемым объектом;
- испытания несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);
- формирование программ и методик аттестационных испытаний;
- разработку заключения договоров на аттестацию;
- проведение аттестационных испытаний объекта информатизации;
- оформление, регистрацию и выдачу «Аттестата соответствия»;
- осуществление государственного контроля и надзора, инспекционного контроля проведения аттестации и эксплуатации аттестованных объектов информатизации;

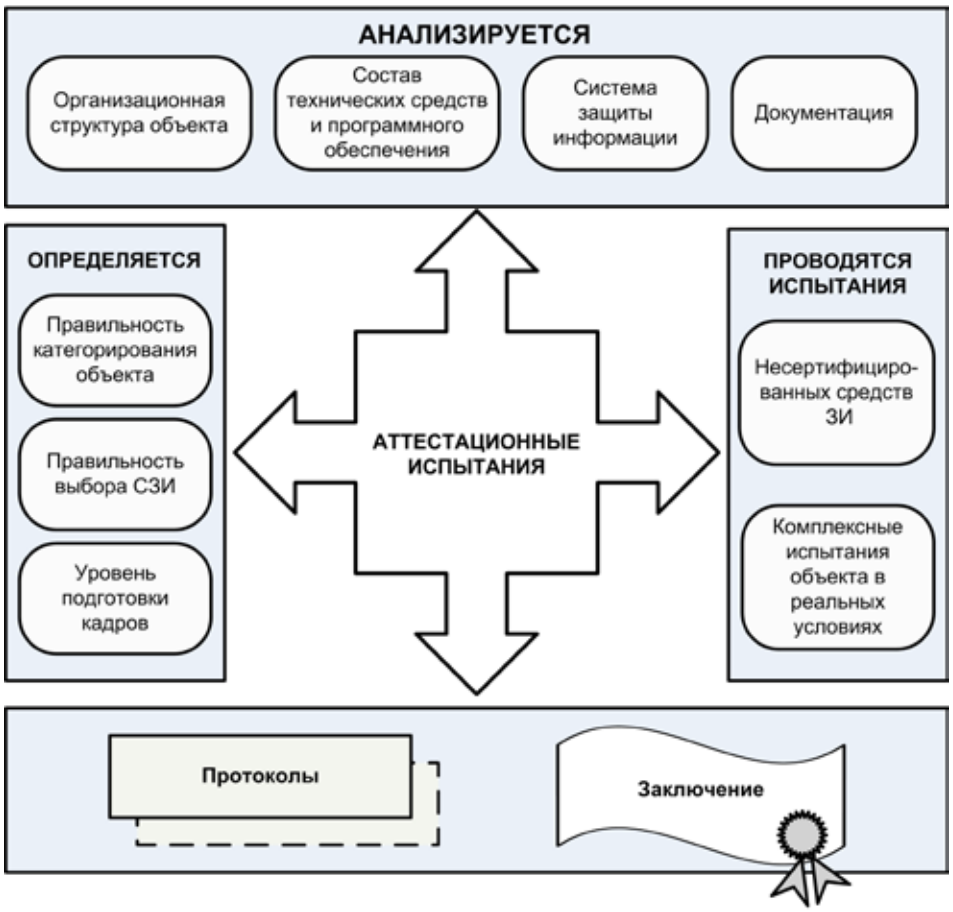

Рис. 1. Порядок проведения аттестационных испытаний

• рассмотрение апелляций.

Порядок применения процедуры аттестации, формы аттестатов соответствия определены в соответствующих нормативных документах [4].

Испытательные центры (лаборатории) сертификации продукции по требованиям безопасности информации по заказам заявителей проводят испытания несертифицированной продукции, используемой на ОИ, подлежащем обязательной аттестации, в соответствии с [8].

Аттестация продукта или системы информационных технологий (ИТ) является административным процессом, посредством которого предоставляются полномочия на их использование в конкретной среде эксплуатации. Оценка концентрируется на тех аспектах безопасности продукта или системы ИТ и на тех аспектах среды эксплуатации, которые могут непосредственно влиять на безопасное использование элементов ИТ. Результаты процесса оценки являются, следовательно, важными исходными материалами для процесса аттестации. Однако, поскольку для оценки не связанных с ИТ характеристик безопасности продукта или системы, а также их соотнесения с аспектами безопасности ИТ более приемлемы другие способы, аттестующим целесообразно предусмотреть для этих аспектов особый подход.

Государственный контроль и надзор, инспекционный контроль аттестации объектов информатизации осуществляется ФСТЭК России как в процессе, так и по завершении аттестации, а контроль эксплуатации аттестованных ОИ проводится периодически в соответствии с планами работы по контролю и надзору.

ФСТЭК России может передавать некоторые из своих функций государственного контроля и надзора за аттестацией и эксплуатацией аттестованных ОИ аккредитованным органам по аттестации.

Объем, содержание и порядок государственного контроля и надзора устанавливаются в нормативной и методической документации по аттестации ОИ.

По результатам анализа нормативных документов, регламентирующих процедуру сертификации средств защиты информации и аттестации объектов информатизации, можно сделать вывод о том, что система аттестации имеет аналогичную системе сертификации организационную структуру и существенное отличие процедуры аттестации от сертификации в области защиты информации состоит лишь в масштабах объекта оценки.

Интересно, что в международных стандартах, определяющих методологию оценки безопасности информационных технологий и АС [13, 14], отсутствует условное деление процедуры оценки соответствия в области защиты информации на сертификацию и аттестацию. В США сертификация по требованиям безопасности — это проводимый независимыми экспертами комплекс организационно-технических мероприятий по проверке соответствия реализованных в АС или СВТ механизмов безопасности определенному набору требований. Требования безопасности используются в качестве критерия для оценки уровня защищенности АС или СВТ. Они могут быть сформулированы в руководящих документах органов государственного управления, внутриведомственных и межведомственных приказах, национальных и международных стандартах, стандартизированных профилях защиты или заданиях по безопасности, а также в виде требований конкретной организации или пользователей АС.

Таким образом, по мнению авторов, существующее условное деление на систему сертификации и систему аттестации в области защиты информации в настоящее время теряет свою актуальность и вводит в заблуждение относительно применяемой терминологии.

В связи с этим целесообразно рассматривать процедуру сертификации как единственную форму подтверждения соответствия в области защиты информации, масштабируемую в зависимости от объекта оценки, а аттестационные комиссии рассматривать как выездные испытательные лаборатории системы сертификации.

В таком случае появляются следующие возможности:

- использовать процедуру сертификации для подтверждения соответствия объектов любого масштаба и сложности;
- исключить разные толкования используемых терминов;
- использовать общие подходы к анализу и синтезу системы подтверждения соответствия;
- оформлять результаты процедуры (сертификации и аттестации в современном понятии) в виде однотипных документов.

Анализ процесса функционирования системы сертификации, представленный на рисунке 2, дает возможность представить ее в виде совокупности системы массового обслуживания (СМО) с испытательными лабораториями в качестве обслуживающих приборов и системы распознавания образов (СРО), реализующей процедуру оценки соответствия требованиям (эталонам) безопасности информации на основе данных от испытательных лабораторий [11].

Объединение сертификации и аттестации в единую процедуру дает возможность представить всю совокупность заявок на сертификацию и аттестацию как один поток заявок на сертификацию по требованиям безопасности информации.

Моделирование системы сертификации как системы массового обслуживания дает возможность решить следующие задачи:

1. Синтез параметров системы по заданным характеристикам входного потока заявок, тре-

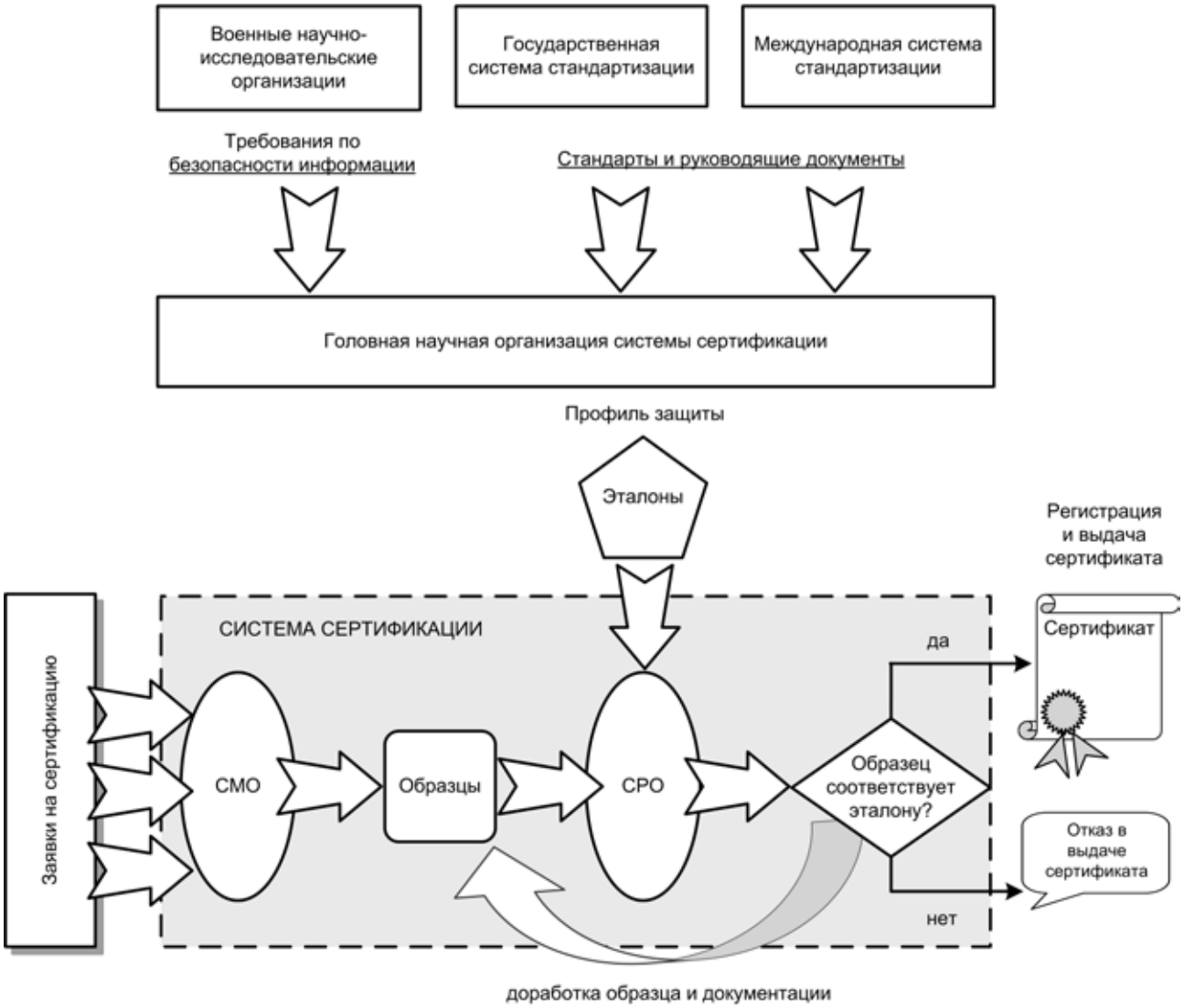

Рис. 2. Процесс функционирования системы сертификации

буемому качеству обслуживания, способу (дисциплине) обслуживания.

2. Обоснование специализации испытательных лабораторий по видам проводимых испытаний, требуемому количеству лабораторий.

3. Оптимизация минимальных параметров системы по заданному качеству, дисциплине обслуживания, характеристикам входящего потока заявок.

4. Оптимизация параметров системы, при которых качество обслуживания максимально для заданных характеристик входящего потока заявок и дисциплины обслуживания.

5. Анализ качества обслуживания системой сертификации потока заявок на сертификацию.

Моделирование системы сертификации, с точки зрения теории распознавания, заключается в представлении результатов испытаний, проводимых в сертификационных лабораториях, как признаков, свойственных объектам распознавания (сертификации). Орган сертификации в этом случае определяет по этим признакам степень сходства объекта с эталоном (профилем защиты).

По результатам распознавания принимается либо положительное решение о выдаче сертификата соответствия, либо отказ при несоответствии объекта предъявляемым требованиям (эталону).

Рассмотренный авторами подход дает возможность обосновать показатели эффективности системы сертификации как системы распознавания и решить следующие задачи:

1. Разработка профилей защиты (эталонов) для АС.

2. Создание методик обработки результатов испытаний.

3. Обоснование перечня наиболее информативных и независимых признаков сертифицируемого объекта.

4. Обоснование срока действия сертификата соответствия.

5. Обоснование надежности сертификата соответствия (вероятности ошибок 1-го и 2-го рода).

6. Оценка надежности информационной системы в условиях ненадежности отдельных ее элементов.

Необходимо отметить, что наблюдаемая интеграция государственной системы в международную систему сертификации не допустима по требованиям безопасности информации.

Главной целью сертификации средств защиты информации (СЗИ) и АС в защищенном исполнении является оценка соответствия требованиям по безопасности информации с заданной точностью и достоверностью для обеспечения заданного качества защиты информации.

Эта задача противоположна задаче, выполняемой разведкой. Так как существуют значительные различия в моделях вероятного противника для каждого государства, то известные международные стандарты по безопасности информации требуют адаптации и ограниченного согласования с отечественными стандартами.

Разработка системы показателей и критериев эффективности сертификации в области защиты информации является актуальной научной задачей.

В настоящее время мероприятия по контролю эффективности защиты информации подразделяются на организационные и технические. Однако не совсем понятно как эти мероприятия соотносятся с аттестацией ОИ и сертификацией СЗИ. Совсем другое дело, если под контролем эффективности понимается государственный надзор (контроль), который осуществляется в области защиты информации ФСТЭК России.

Согласно Положению о лицензировании в области защиты информации:

эффективность защиты информации — степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты;

контроль эффективности защиты информации — проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты.

В ГОСТ 50922-2006 даны следующие определения:

эффективность защиты информации — степень соответствия результатов защиты информации поставленной цели;

показатель эффективности защиты информации — мера или характеристика для оценки эффективности защиты информации;

контроль эффективности защиты информации — проверка соответствия качественных и количественных показателей эффективности мероприятий по защите информации требованиям или нормам эффективности защиты информации.

В соответствии со стандартом ГОСТ Р ИСО 9000-2008:

эффективность — связь между достигнутым результатом и использованными ресурсами;

результативность — степень реализации запланированной деятельности и достижения запланированных результатов;

качество — степень соответствия присущих характеристик требованиям.

Исходя из этого, следует понимать, что сертификация по требованиям безопасности информации (как масштабируемая процедура) направлена на *оценку качества средств (систем) защиты информации и оценку результативности мероприятий по защите информации.*

Заключение

В результате приведенных рассуждений можно сделать следующие выводы:

1. Разделение системы подтверждения соответствия в области защиты информации на сер-

тификацию и аттестацию является условным. Во избежание противоречий вместо аттестации объектов информатизации целесообразно использовать только понятие сертификации как масштабируемой процедуры подтверждения соответствия.

2. Рассмотрен новый подход к процедуре сертификации в области защиты информации, позволяющий обосновать количественные показатели эффективности системы сертификации.

3. Обоснована применимость математического аппарата, теории массового обслуживания и теории распознавания образов для описания процесса функционирования системы сертификации.

4. Нецелесообразно интегрировать государственную систему сертификации по требованиям безопасности информации в международную систему сертификации.

5. Современное понятие эффективности защиты информации эквивалентно ее результативности в международной терминологии.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации : утв. Президентом РФ 09.09.2000.

2. ГОСТ 16504-81. Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения : [с измен. № 1 от 10.10.2003]. — М. : ИПК Изд-во стандартов, 2004

3. ГОСТ 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. — М. : Стандартинформ, 2007.

4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. — М. : Стандартинформ, 2008.

5. ГОСТ Р ИСО 9001-2008. Системы менеджмента качества. Требования. — М. : Стандартинформ, 2009.

6. Положение о государственном лицензировании деятельности в области защиты информации от 27.04.1994 г.

7. Положение по аттестации объектов информатизации по требованиям безопасности информации от 25.11.1994 г.

8. Положение о сертификации средств защиты информации по требованиям безопасности информации от 26.06.1995 г.

9. Максимов Р. В. Технические средства и методы защиты информации. Ч. 1 / Р. В. Максимов, А. В. Павловский. — СПб. : СПбГЭТУ, 2001.

10. Соснин П. И. Материализация требований информационной безопасности в разработке автоматизированных систем / П. И. Соснин, В. С. Жуков // Материалы Всероссийской конференции «Проведение научных исследований в области обработки, хранения, передачи и защиты информации». Т. 2. — Ульяновск : УлГТУ, 2009. — С. 76—84.

11. Стародубцев Ю. И. Соотношение сертификации и аттестации в области защиты информации / Ю. И. Стародубцев, Ю. К. Худайназаров // Материалы IV Международной научной конференции «Исследование, разработка и применение высоких технологий в промышленности». — СПб. , 2007. — С. 124—132.

12. О техническом регулировании : федер. закон № 184-ФЗ : принят Гос. Думой 15.12.2002 : [ред. от 30.12.2009].

13. ISO/IEC 15408. Common Criteria for Information Technology Security Evaluation Part 1—3 Version 3.0, June 2005.

14. ISO/IEC 19791: 2006 Information technology — Security techniques — Security assessment of operational systems.