Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

В. Ф. Голиков, И. И. Черная, О. Б. Зельманский

МЕТОЛОГИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рекомендовано УМО по образованию
В области информатики и радиоэлектроники
В качестве учебно-методического пособия для студентов учреждений,
обеспечивающих получение высшего образования
по 2-й ступени высшего образования по специальности
1-40 80 01 «Методы системы защиты
Информации, информационная безопасность»

Минск БГУИР 2012

УДК 004.056.5(075.8)
ББК 32.973.26-018.2я73
Г60

Р е ц е н з е н т :

кафедра «Информационные системы и технологии»
Белорусского национального технического университета
(протокол №2 от 15.10.2011г.);

начальник сектора унитарного предприятия «Научно-исследовательский институт средств автоматизации», кандидат технических наук В. А. Апорович

заведующий кафедрой телекоммуникационных систем Высшего государственного колледжа связи,
кандидат технических наук, доцент К. И. Пирогов

Голиков, В. Ф.

Г60 Методологические основы информационной безопасности : учеб.-метод. пособие / В. Ф. Голиков, И. И. Черная, О. Б. Зельманский. – Минск : БГУИР, 2012. – 72 с.

ISBN 978-985-488-614-5.

В пособии рассмотрены методологические основы информационной безопасности на современном этапе. Разработаны и сформулированы основные принципы методологии создания и обеспечения безопасности информации, а также приведены примеры формирования профилей защиты.

Предназначено для студентов второй ступени высшего образования дневной и заочной форм обучения по специальности 1-40 80 01 «Методы и системы защиты информации, информационная безопасность»

УДК 004.056.5(075.8)
ББК 32.973.26-18.2я73

ISBN 978-985-488-614-5

СПИСОК УСЛОВНЫХ СОКРАЩЕНИЙ

АС – автоматизированная система

ВЧС – виртуальная частная сеть

ГТБ – гарантийные требования к безопасности

ЗБ – задание по безопасности

ЗИ – защита информации

ИБ – информационная безопасность

ИС – информационная система

ИТ – информационные технологии

КСБ – конфигурация системы безопасности

ОК – «Общие критерии оценки безопасности информационных технологий»

ОО – объект оценки

ПБ – политика безопасности

ПД – поддержка доверия

ПЗ – профиль защиты

СБ – средства безопасности

СБОО – средства безопасности объекта оценки

СВТ – средства вычислительной техники

СО – субъект оценки

УГО – уровень гарантии оценки

УК – управление конфигурацией

ФБ – функции безопасности

ФП – функциональные пакеты

Содержание

Введение

Современный этап развития и применения информационных технологий характеризуется острой необходимостью в разработке и создании комплексных систем обеспечения безопасности информации, позволяющих надежно хранить, обрабатывать и передавать информацию потребителям.

Проблема защиты информации в сегодняшнем обществе – это многогранная проблема сохранения важнейшего ресурса этого общества – информационного ресурса.

Это выдвигает на первый план задачу создания и разработки методологических основ обеспечения информационной безопасности. Данное учебно-методическое пособие представляет собой попытку восполнить некоторый пробел в этой области.

Предлагаемая концепция методологии информационной безопасности базируется на основных законах, регламентирующих юридические аспекты обеспечения безопасности информации и международном опыте создания защищенных систем.

Рассмотрены методологические аспекты систем обеспечения информационной безопасности, включающие терминологию, общую модель и общие критерии оценки безопасности информационных технологий.

Описаны классы функциональных требований безопасности и требования доверия безопасности на всех этапах разработки и эксплуатации изделий. Приведены примеры формирования профилей защиты.

1. Проблемы создания защищенных систем

1.1. Проблемы создания защищенных систем на современном этапе

Как и всякая другая наука, наука о защите информации (ЗИ) развивается двумя путями: от частного к общему и от общего к частному. Разрабатывая и используя те или иные методы и средства защиты, специалисты уже с 80-х годов XX в. пытались ответить на основные вопросы: что такое защищенная информационная система? как задать и измерить уровень защищенности? Без правильного ответа на эти вопросы невозможно рассматривать основные принципы функционирования подобных систем и технологию их создания. Так как защищенность (безопасность) является качественной характеристикой системы, то сложно сравнивать то или иное решение без определенных критериев сравнения. Эти критерии должны быть узаконены в виде стандартов информационной безопасности (ИБ). Эти документы должны регламентировать основные понятия и концепции ИБ на государственном или межгосударственном уровне, определять само понятие защищенной системы посредством стандартизации требований и критериев безопасности, образующих шкалу оценки степени защищенности.

Главная задача методологии ИБ, оформленной в виде стандартов, – создать основу для взаимодействия между производителями, потребителями и экспертами с целью создания защищенных информационных систем (ИС).

1.2. История развития методологии

Общая методология ЗИ последовательно излагалась в следующих документах:

1. Критерии безопасности компьютерных систем Министерства обороны США.
2. Руководящие документы Гостехкомиссии России.
3. Европейские критерии безопасности ИТ.
4. Федеральные критерии безопасности ИТ США.
5. Канадские критерии безопасности компьютерных систем.
6. Общие критерии безопасности ИТ.

Первым оценочным стандартом, получившим международное признание и оказавшим исключительно сильное влияние на последующие разработки в области ИБ, стал *стандарт* Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Department of Defense Trusted Computer

System Evaliation Criteria, TCSEC), более известный (по цвету обложки) под названием *«Оранжевая книга»* (1983).

В «Оранжевой книге» заложен понятийный базис ИБ. Достаточно лишь перечислить содержащиеся в нем понятия: *безопасная* и *доверенная системы*, *политика безопасности*, *уровень гарантированности*, *подотчетность*, *доверенная вычислительная база*, *монитор обращений*, *ядро* и *периметр безопасности*. Исключительно важно также выделение таких аспектов политики безопасности, как добровольное (*дискреционное*) и *принудительное (мандатное) управление доступом*, *безопасность повторного использования объектов*. После «Оранжевой книги» была выпущена целая *«Радужная серия»*. С концептуальной точки зрения наиболее значимый документ в ней – «*Интерпретация «Оранжевой книги» для сетевых конфигураций*» (Trusted Network Interpretation), разработанный в 1987 году Национальным центром компьютерной безопасности США. Он состоит из двух частей. Первая содержит собственно интерпретацию, во второй описываются *сервисы безопасности*, специфичные или особенно важные для сетевых конфигураций.

Важнейшее понятие, введенное в первой части, – сетевая *доверенная вычислительная база*, которая создается с учетом динамичности сетевых конфигураций. Среди защитных механизмов выделена *криптография*, помогающая поддерживать как *конфиденциальность*, так и *целостность*.

Новым для своего времени стал системный подход к вопросам *доступности*, формирование архитектурных принципов ее обеспечения.

«Гармонизированные критерии Европейских стран» были разработаны в 1991 году специалистами Франции, Германии, Нидерландов и Великобритании.

Формулируется *цель оценки*, затем орган сертификации определяет, насколько полно она достигается, то есть в какой мере корректны и эффективны архитектура и реализация *механизмов безопасности* в конкретной ситуации. Чтобы облегчить формулировку цели оценки, *стандарт* содержит описание десяти примерных классов функциональности, типичных для правительственных и коммерческих систем.

В «Гармонизированных критериях» подчеркивается различие между системами и продуктами ИТ, но для унификации требований вводится единое понятие – *объект оценки*.

Важно указание и на различие между *функциями (сервисами) безопасности* и реализующими их механизмами, а также выделение двух аспектов гарантированности – *эффективности* и *корректности* средств безопасности.

Руководящие документы Гостехкомиссии России начали появляться несколько позже, уже после опубликования «Гармонизированных критериев», и по аналогии с последними подтверждают разницу между автоматизированными системами (АС) и продуктами (средствами вычислительной техники, СВТ), но в общем и целом, эти документы долгое время следовали в фарватере «Оранжевой книги».

1.3. «Оранжевая книга»

Естественно, что такое название документа требует комментария. Речь идет не о безопасных, а о *доверенных системах*, то есть системах, которым можно оказать определенную *степень доверия*.

«Оранжевая книга» поясняет понятие *безопасной системы*, которая «управляет с помощью соответствующих средств доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию».

Очевидно, однако, что *абсолютно* безопасных систем не существует, это абстракция. Есть смысл оценивать лишь *степень доверия*, которое можно оказать той или иной системе.

В «Оранжевой книге» *доверенная система* определяется как «система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа».

Обратим внимание, что в рассматриваемых критериях и безопасность, и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности и целостности (статической).

Вопросы доступности «Оранжевая книга» не затрагивает.

Степень доверия оценивается по двум основным критериям:

1. *Политика безопасности (ПБ)* – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия к системе, тем строже и многообразнее должна быть ПБ. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности – это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

2. *Уровень гарантированности* – мера доверия, которая может быть оказана архитектуре и *реализации* ИС. Доверие к политике безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. *Уровень гарантированности* показывает, насколько корректны механизмы, отвечающие за *реализацию* ПБ. Это пассивный аспект защиты.

Важным средством обеспечения безопасности является механизм *подотчетности* (протоколирования). *Доверенная система* должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть *анализом регистрационной информации*.

Концепция доверенной вычислительной базы является центральной при оценке степени доверия безопасности. *Доверенная вычислительная база* – это совокупность защитных механизмов ИС (включая аппаратное и программное

обеспечение), отвечающих за проведение в жизнь ПБ. Качество вычислительной базы определяется исключительно ее *реализацией* и корректностью исходных данных, которые вводит системный администратор.

Основное *назначение* доверенной вычислительной базы – выполнять функции *монитора обращений*, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

Монитор обращений должен обладать тремя качествами:

1. *Изолированность*. Необходимо предупредить возможность отслеживания работы монитора.

2. *Полнота*. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.

3. *Верифицируемость*. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в *полноте* тестирования.

Реализация монитора обращений называется ядром безопасности. *Ядро безопасности* – это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств *монитора обращений* ядро должно гарантировать собственную неизменность.

Границу доверенной вычислительной базы называют *периметром безопасности*. Как уже указывалось, компоненты, лежащие вне периметра безопасности, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию *«периметр безопасности»* все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне, – нет.

Механизмы безопасности

Согласно «Оранжевой книге», ПБ должна обязательно включать в себя следующие элементы:

- *произвольное управление доступом*;
- *безопасность повторного использования объектов*;
- *метки безопасности*;
- *принудительное управление доступом*.

Произвольное управление доступом (называемое иногда дискреционным) – это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.

Безопасность повторного использования объектов – важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из «мусора». Безопасность повторного использования должна гарантироваться для областей оперативной

памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т. п.), для дисковых блоков и магнитных носителей в целом.

Как указывалось ранее, современный объектно-ориентированный подход резко сужает область действия данного элемента безопасности, затрудняет его реализацию. То же верно и для интеллектуальных устройств, способных буферизовать большие объемы данных.

Для реализации принудительного управления доступом с субъектами и объектами ассоциируются *метки безопасности*: метка субъекта описывает его благонадежность, метка объекта – степень конфиденциальности содержащейся в нем информации.

Согласно «Оранжевой книге», *метки безопасности* состоят из двух частей – уровня секретности и списка категорий. Уровни секретности образуют упорядоченное множество, категории – неупорядоченное. Назначение последних – описать предметную область, к которой относятся данные.

*Принудительное (*или *мандатное) управление доступом* основано на сопоставлении *меток безопасности субъекта* и *объекта*.

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка *субъекта* доминирует над меткой *объекта*. Это означает: читать можно только то, что положено.

Субъект может записывать информацию в объект, если метка безопасности *объекта* доминирует над меткой *субъекта*. В частности, «конфиденциальный» субъект может записывать данные в секретные файлы, но не может – в несекретные (разумеется, должны также выполняться ограничения на набор категорий).

Описанный способ управления доступом называется *принудительным*, поскольку он не зависит от воли субъектов (даже системных администраторов). После того как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа.

Если понимать ПБ узко, то есть как правила разграничения доступа, то механизм *подотчетности* является дополнением подобной политики. *Цель* подотчетности – в каждый момент времени знать, кто работает в системе и что там делает. *Средства* подотчетности делятся на три категории:

- *проверка подлинности (идентификация* и *аутентификация)*;
- *предоставление доверенного пути*;
- *анализ регистрационной информации*.

Обычный способ идентификации – *ввод имени пользователя при входе в систему*. Стандартное средство проверки подлинности (аутентификации) пользователя – *пароль*.

Доверенный путь связывает пользователя непосредственно с *доверенной вычислительной базой*, минуя другие потенциально опасные компоненты ИС. *Цель* предоставления доверенного пути – дать пользователю возможность убедиться в подлинности обслуживающей его системы.

Анализ регистрационной информации (аудит) имеет дело с действиями (событиями), так или иначе затрагивающими безопасность системы.

Если фиксировать все события, объем регистрационной информации скорее всего будет расти слишком быстро, а ее эффективный анализ станет невозможным. «Оранжевая книга» предусматривает наличие средств выборочного протоколирования как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.

Переходя к пассивным аспектам защиты, укажем, что в «Оранжевой книге» рассматриваются два вида гарантированности – операционная и технологическая. *Операционная гарантированность* относится к архитектурным и реализационным аспектам системы, в то время как *технологическая* – к методам построения и сопровождения.

Операционная гарантированность включает в себя проверку следующих элементов:

- архитектуры системы;
- целостности системы;
- тайных каналов передачи информации;
- доверенного администрирования;
- доверенного восстановления после сбоев.

Операционная гарантированность – это способ убедиться в том, что архитектура системы и ее *реализация* действительно соответствуют избранной *политике безопасности*.

Технологическая гарантированность охватывает весь *жизненный цикл ИС*, т. е. периоды *проектирования*, *реализации*, *тестирования*, *продажи* и *сопровождения*. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и нелегальные «закладки».

Классы безопасности

«Критерии ...» МО США открыли путь к ранжированию информационных систем по *степени доверия* безопасности.

В «Оранжевой книге» определяются четыре уровня доверия – D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к системам предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием степени доверия.

Всего имеется шесть *классов безопасности* – C1, C2, B1, B2, B3, A1. Чтобы в результате процедуры сертификации систему можно было отнести к некоторому классу, ее ПБ и уровень гарантированности должны удовлетворять заданным требованиям, из которых упомянем лишь важнейшие.

Класс C1:

- доверенная вычислительная база должна управлять доступом именованных пользователей к именованным объектам;
- пользователи должны идентифицировать себя, прежде чем выполнять какие-либо иные действия, контролируемые доверенной вычислительной базой.

Для аутентификации должен использоваться какой-либо защитный механизм, например, пароли. Аутентификационная информация должна быть защищена от несанкционированного доступа;

- доверенная вычислительная база должна поддерживать область для собственного выполнения, защищенную от внешних воздействий (в частности, от изменения команд и/или данных) и от попыток слежения за ходом работы;
- должны быть в наличии аппаратные и/или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов доверенной вычислительной базы;
- защитные механизмы *должны быть протестированы* на предмет соответствия их поведения системной документации. Тестирование должно подтвердить, что у неавторизованного пользователя нет очевидных способов обойти или разрушить средства защиты доверенной вычислительной базы;
- должны быть описаны подход к безопасности, используемый производителем, и применение этого подхода при реализации доверенной вычислительной базы.

Класс С2 (в дополнение к С1):

- права доступа должны гранулироваться с точностью до пользователя. Все объекты должны подвергаться контролю доступа;
- при выделении хранимого объекта из пула ресурсов доверенной вычислительной базы необходимо ликвидировать все следы его использования;
- каждый пользователь системы должен уникальным образом идентифицироваться. Каждое регистрируемое действие должно ассоциироваться с конкретным пользователем;
- доверенная вычислительная база должна создавать, поддерживать и защищать журнал регистрационной информации о доступе к объектам, контролируемым базой;
- тестирование должно подтвердить отсутствие очевидных недостатков в механизмах изоляции ресурсов и защиты регистрационной информации.

Класс В1 (в дополнение к С2):

- доверенная вычислительная база должна управлять метками безопасности, ассоциируемыми с каждым субъектом и хранимым объектом;
- доверенная вычислительная база должна обеспечить реализацию принудительного управления доступом всех субъектов ко всем хранимым объектам;
- доверенная вычислительная база должна обеспечивать взаимную *изоляцию процессов* путем *разделения* их *адресных пространств*;
- группа специалистов, отвечающих за реализацию доверенной вычислительной базы, должна подвергнуть описание архитектуры, исходные и объектные коды тщательному анализу и тестированию;
- должна существовать неформальная или формальная модель ПБ, поддерживаемая доверенной вычислительной базой.

Класс B2 (в дополнение к B1):

- снабжаться метками должны все ресурсы системы (например ПЗУ), прямо или косвенно доступные субъектам;
- к доверенной вычислительной базе должен поддерживаться доверенный коммуникационный *путь* для пользователя, выполняющего операции начальной идентификации и аутентификации;
- должна быть предусмотрена возможность регистрации событий, связанных с организацией тайных каналов обмена с памятью;
- доверенная вычислительная база должна быть внутренне структурирована на правильно определенные, относительно независимые модули;
- администратор безопасности должен тщательно проанализировать возможности организации тайных каналов обмена с памятью и оценить максимальную пропускную способность каждого выявленного канала;
- должна быть продемонстрирована относительная устойчивость доверенной вычислительной базы к попыткам проникновения;
- модель ПБ должна быть формальной. Для доверенной вычислительной базы должны существовать описательные спецификации верхнего уровня, точно и полно определяющие ее интерфейс. Спецификация определяет отображение требований на функции безопасности (ФБ), при этом предусматривается наличие нескольких уровней представления проекта с его декомпозицией и детализацией. Выделяют формальную и функциональную спецификации;
- в процессе разработки и *сопровождения* доверенной вычислительной базы должна использоваться система конфигурационного управления, обеспечивающая контроль изменений в описательных спецификациях верхнего уровня, иных архитектурных данных, реализационной документации, исходных текстах, работающей версии объектного кода, тестовых данных и документации;
- тесты должны подтверждать действенность мер по *уменьшению* пропускной способности тайных каналов передачи информации.

Класс B3 (в дополнение к B2):

- для *произвольного управления доступом* должны обязательно использоваться *списки управления доступом* с указанием разрешенных режимов;
- должна быть предусмотрена возможность регистрации появления или накопления событий, несущих угрозу ПБ системы. *Администратор безопасности* должен немедленно извещаться о попытках нарушения ПБ, а система в случае продолжения попыток сама должна пресекать их наименее болезненным способом;
- доверенная вычислительная база должна быть спроектирована и структурирована таким образом, чтобы использовать полный и концептуально простой защитный механизм с точно определенной семантикой;
- процедура анализа должна быть выполнена для временных тайных каналов;

- должна быть специфицирована роль администратора безопасности. Получить права администратора безопасности можно только после выполнения явных, протоколируемых действий;
- должны существовать процедуры и/или механизмы, позволяющие произвести восстановление после сбоя или после иного нарушения работы без ослабления защиты;
- должна быть продемонстрирована устойчивость доверенной вычислительной базы к попыткам проникновения.

Класс А1 (в дополнение к В3):

- тестирование должно продемонстрировать, что реализация доверенной вычислительной базы соответствует формальным спецификациям верхнего уровня;
- помимо описательных, должны быть представлены формальные спецификации верхнего уровня. Необходимо использовать современные методы формальной спецификации и *верификации* систем;
- механизм конфигурационного управления должен распространяться на весь жизненный цикл и все компоненты системы, имеющие отношение к обеспечению безопасности;
- должно быть описано соответствие между формальными спецификациями верхнего уровня и исходными текстами.

Такова классификация, введенная в «Оранжевой книге». Коротко ее можно сформулировать так:

- уровень С – *произвольное управление доступом*;
- уровень В – *принудительное управление доступом*;
- уровень А – *верифицируемая безопасность*.

Конечно, в адрес «Критериев ...» можно высказать целый ряд серьезных замечаний (таких, например, как полное игнорирование проблем, возникающих в распределенных системах). Тем не менее, следует подчеркнуть, что публикация «Оранжевой книги» без всякого преувеличения стала эпохальным событием в области ИБ. Появился общепризнанный понятийный базис, без которого даже обсуждение проблем ИБ было бы затруднительным.

Отметим, что огромный идейный потенциал «Оранжевой книги» пока во многом остается невостребованным. Прежде всего, это касается концепции *технологической гарантированности*, охватывающей весь *жизненный цикл системы* – от выработки спецификаций до фазы эксплуатации. При современной технологии программирования результирующая система не содержит информации, присутствующей в исходных спецификациях, теряется информация о семантике программ.

1.4. Контрольные вопросы

1. В чем заключается главная задача методологии информационной безопасности?

2. Что такое «доверенная система»?

3. В каком оценочном стандарте заложен понятийный базис информационной безопасности?

4. По каким двум основным критериям оценивается степень доверия? Что они собой представляют?

5. Что такое «доверенная вычислительная база» и из чего она состоит?

6. Какие виды гарантированности вы знаете?

7. Перечислите известные вам классы безопасности.

2. Общие критерии. Описание модели

2.1. История создания и текущий статус «Общих критериев»

В 1990 году Международная организация по стандартизации (ISO) приступила к разработке «*Критериев оценки безопасности информационных технологий*» (Evaluation Criteria for IT Security, ECITS). Несколько позже, в 1993 году, правительственные организации шести североамериканских и европейских стран – Канады, США, Великобритании, Германии, Нидерландов и Франции – занялись составлением так называемых «*Общих критериев оценки безопасности информационных технологий*» (Common Criteria for IT Security Evaluation). За этим документом исторически закрепилось более короткое название – «*Общие критерии*», или ОК (Common Criteria, CC).

В ОК требовалось объединить и развить всего три весьма продвинутых и близких по духу документа – «Гармонизированные критерии Европейских стран», «Канадские критерии оценки доверенных компьютерных продуктов» и «Федеральные критерии безопасности информационных технологий» (США). (Сами разработчики «Общих критериев» относят к числу первоисточников еще и «Оранжевую книгу».) В 1996 году появилась версия 1.0 «Общих критериев», которая, помимо публикации в Internet для всеобщего свободного доступа, была одобрена ISO и обнародована в качестве проекта комитета.

Широкое открытое обсуждение документа и его реализация привели к существенной переработке первоначальной версии и выходу версии 2.0 «ОК» в мае 1998 года. С целью унификации процедуры сертификации по «Общим критериям» в августе 1999 года была опубликована «*Общая методология оценки безопасности информационных технологий*» (Common Methodology for Information Technology Security Evaluation), описывающая минимальный набор действий при проведении оценки. «Проект ОК» с самого начала носил не только технический, но и экономико-политический характер. Его цель состояла, в частности, в том, чтобы упростить, удешевить и ускорить выход сертифицированных изделий информационных технологий (ИТ) на мировой рынок. Изделие ИТ – собирательный термин для обозначение систем и продуктов ИТ. Для этого в мае 2000 года уполномоченные правительственные организации шести стран-основателей «Проекта ОК», а также Австралии и Новой Зеландии, Греции, Италии, Испании, Норвегии, Финляндии и Швеции подписали соглашение *«О признании сертификатов по* «*Общим критериям в области безопасности информационных технологий*» (позднее к нему присоединились Австрия и Израиль).

Участие в соглашении предполагает соблюдение двух независимых условий: признание *сертификатов*, выданных соответствующими органами других стран-участниц, а также возможность осуществления подобной сертификации в стране-подписанте. Очевидно, от взаимного признания сертификатов выигрывают не только производители, но и потребители изделий ИТ. Что же касается их выдачи, то соглашение предусматривает жесткий контроль при получении и

подтверждении этого права (например, предусмотрено проведение так называемых теневых сертификационных испытаний под контролем независимых экспертов). Таким образом, для полноценного участия в соглашении, помимо желания, государство должно располагать органами сертификации с достаточными ресурсами и штатом специалистов, квалификация которых получила официальное международное признание. По данным на конец 2002 года правом выдачи *сертификатов*, признаваемых участниками соглашения, обладали Австралия и Новая Зеландия, Великобритания, Германия, Канада, США и Франция.

К началу 2003 года сертификаты по «Общим критериям» получили около семидесяти разнообразных изделий ИТ ведущих производителей: операционные системы, системы управления базами данных, межсетевые экраны, коммуникационные средства, интеллектуальные карты и т. п.; еще почти сорок находились в процессе сертификации.

Республика Беларусь осуществила самостоятельный перевод текста «ОК» и ввела «Общие критерии» сначала в качестве предстандарта, а с 2004 г. – в качестве государственного стандарта. Официальные названия стандартов:

1. СТБ 34.101.1-2004(ИСО/МЭК 15408-1:1999). Информационные технологии и безопасность.

Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

2. СТБ 34.101.2-2004(ИСО/МЭК 15408-2:1999). Информационные технологии и безопасность.

Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

3. СТБ 34.101.3-2004(ИСО/МЭК 15408-3:1999). Информационные технологии и безопасность.

Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности.

К сожалению, в 2010 г. Республика Беларусь еще не может полноценно участвовать в соглашении «О признании сертификатов по «Общим критериям в области безопасности информационных технологий»», поскольку не располагает органами сертификации с достаточными ресурсами и штатом специалистов, квалификация которых получила официальное международное признание.

2.2. Основные понятия и идеи «Общих критериев»

Основным свойством, которым должны обладать действительно *общие критерии* оценки безопасности ИТ, является универсальность. Следовательно, они не должны содержать априорных предположений об *объекте оценки*. В «ОК» данное условие выполнено: под *объектом оценки* (ОО) понимается аппа-

ратно-программный *продукт* или информационная *система* (наряду с руководством администратора и пользователя), включающая в себя такие ресурсы, как электронные запоминающие устройства (например диски), периферийные устройства (например принтеры) и вычислительную мощность (например процессорное время), которые могут быть использованы для обработки и хранения информации.

Система – это специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

Продукт, согласно «ОК», есть совокупность средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы. Как упоминалось выше, в качестве собирательного термина для систем и продуктов применяют словосочетание «*изделие ИТ*». Оно может быть как уже существующим, так и проектируемым. В первом случае – доработано по результатам оценки, во втором – сама перспектива подобного контроля способна дисциплинировать разработчиков; так или иначе проведение оценки должно оказать положительное влияние на безопасность ОО.

Объект оценки рассматривается в определенном контексте – *среде безопасности*, в которую включаются, что имеет отношение к его безопасности, а именно:

- законодательная среда – законы и нормативные акты, затрагивающие ОО;
- административная среда – положения политики и программ безопасности, учитывающие особенности ОО;
- процедурная среда – физическая среда ОО и меры физической защиты, персонал и его свойства (знания, опыт и т. п.), принятые эксплуатационные и иные процедуры;
- программно-техническая среда – предназначение ОО и предполагаемые области его применения, активы (ресурсы), которые требуют защиты средствами ОО.

Дальнейший этап технологического цикла подготовки к оценке, согласно «*Общим критериям*», – описание следующих аспектов среды ОО:

- *предположения безопасности*. Они выделяют ОО из общего контекста, задают границы рассмотрения. Истинность этих предположений принимается без доказательства, а из множества возможных отбирается только то, что заведомо необходимо для обеспечения безопасности ОО;
- *угрозы безопасности* ОО, наличие которых в рассматриваемой среде установлено или предполагается. Они характеризуются несколькими параметрами: источник, метод воздействия, уязвимые с точки зрения злонамеренного использования объекты, ресурсы (активы), потенциально подверженные повреждению. При анализе рисков принимаются во внимание вероятность активизации угрозы и ее успешного осуществления, а также размер возможного ущерба. По результатам анализа из множества допустимых угроз отбираются только те, ущерб от которых нуждается в уменьшении;

- положения ПБ, предназначенные для применения к ОО. Для системы ИТ такие положения могут быть описаны точно, для продукта – в общих чертах.

На основании предположений при учете угроз и положений ПБ формулируются цели безопасности для ОО, направленные на обеспечение противостояния угрозам и выполнение ПБ. В зависимости от непосредственного отношения к ОО или к среде эти цели подразделяются на две группы. Часть целей для среды может достигаться нетехническими (процедурными) мерами. Все остальные (для объекта и среды) носят программно-технический характер. Для их достижения к объекту и среде предъявляются *требования безопасности*.

«*Общие критерии*» в главной своей части как раз и являются каталогом (библиотекой) требований безопасности. Спектр стандартизованных требований чрезвычайно широк – это необходимое условие универсальности ОК. Высокий уровень детализации делает их конкретными, допускающими однозначную проверку, что важно для обеспечения повторяемости результатов оценки. Наличие параметров обуславливает гибкость требований, а дополнительную возможность ее достижения (через расширяемость) привносит использование нестандартных (не входящих в каталог «ОК») требований.

Для структуризации пространства требований в «*Общих критериях*» введена иерархия *класс–семейство–компонент–элемент*.

Классы определяют наиболее общую (как правило, предметную) группировку требований.

Семейства в пределах *класса* различаются по строгости и другим характеристикам требований.

Компонент – минимальный набор требований, фигурирующий как целое.

Элемент – неделимое требование.

Между компонентами могут существовать зависимости. Они возникают, когда компонент сам по себе недостаточен для достижения цели безопасности. Соответственно при включении такого компонента необходимо навесить на него всю «гроздь» его зависимостей.

«*Общие критерии*» содержат *два* основных *вида* требований безопасности:

- *функциональные*, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности ОО и реализующим их механизмам;
- *требования доверия*, которые соответствуют пассивному аспекту, предъявляются к технологии и процессу разработки и эксплуатации ОО.

Библиотека *функциональных требований безопасности* составляет вторую часть «*Общих критериев*», а каталог *требований доверия* – третью (первая часть содержит изложение основных концепций «ОК»).

Сформулировав функциональные требования, требования доверия и требования к среде, можно приступать к оценке безопасности готового изделия ИТ. Для типовых изделий «*Общие критерии*» предусматривают разработку типовых совокупностей требований безопасности, называемых *профилями защиты* (ПЗ).

Для проектируемого изделия за выработкой требований следует разработка *краткой спецификации*, входящей в *задание по безопасности* (ЗБ).

В качестве вспомогательного *элемента*, упрощающего созданием *профилей защиты* и ЗБ, могут применяться *функциональные пакеты* (ФП) – неоднократно используемые совокупности компонентов, объединенных для достижения установленных целей безопасности.

Краткая спецификация, как было упомянуто выше, определяет отображение требований на ФБ. «*Общие критерии*» не предписывают конкретной методологии или дисциплины разработки изделий ИТ, но предусматривают наличие нескольких уровней представления проекта с его декомпозицией и детализацией. За требованиями безопасности следует *функциональная спецификация*, затем *проект верхнего уровня*, необходимое число промежуточных уровней, *проект нижнего уровня*, после этого в зависимости от типа изделия исходный код или схемы аппаратуры и, наконец, *реализация* в виде исполняемых файлов, аппаратных продуктов и т. п. Между уровнями представления должно демонстрироваться соответствие, т. е. все сущности более высоких уровней обязаны фигурировать и «ниже», а «внизу» нет места лишним сущностям, не обусловленным потребностями более высоких уровней. Таким образом, разработка изделий ИТ включает последовательное создание:

1) требований безопасности;
2) функциональной спецификации;
3) проекта верхнего уровня;
4) проектов промежуточных уровней;
5) проекта нижнего уровня;
6) исходного кода или схемы аппаратуры;
7) реализации.

При проведении оценки изделия ИТ главными являются следующие критерии:

- *соответствие* функций безопасности ОО функциональным требованиям;
- *корректность* реализации функций безопасности.

В случае соответствия изделия обоим критериям можно говорить о достижении целей безопасности.

2.3. Основные понятия и идеи «Общей методологии оценки безопасности информационных технологий»

«Общая методология оценки безопасности информационных технологий» – второй по важности документ (после «Общих критериев»), подготовленный в рамках «Проекта ОК». Основная цель «Общей методологии» – добиться объективности, повторяемости и воспроизводимости результатов оценки.

Следуя принципам структурной декомпозиции, разработчики выделили в процессе оценки три задачи (этапа):

- *входная задача;*

- *задача оценки;*
- *выходная задача.*

Входная задача имеет дело с представленными для оценки свидетельствами (далее для краткости будем именовать их свидетельствами оценки). Ее назначение – убедиться, что версии свидетельств корректны и должным образом защищены.

Обычно для оценки представляются стабильные, официально выпущенные версии свидетельств, однако в ситуациях, когда оценка ведется параллельно разработке или доработке ОО, возможно предъявление рабочих версий. Оценщику вместе со спонсором этого процесса необходимо составить каталог и в дальнейшем производить конфигурационный контроль версий. Оценщик обязан обеспечить защиту свидетельств от изменения и утери, а по окончании процесса оценки возвратить их, поместить в архив или уничтожить.

На всех этапах оценки должна обеспечиваться конфиденциальность.

Задача оценки в общем случае разбивается на следующие подзадачи:

- оценка ЗБ;
- оценка управления конфигурацией ОО;
- оценка документации по передаче ОО потребителю и эксплуатационной документации;
- оценка документации разработчиков;
- оценка руководств;
- оценка поддержки жизненного цикла ОО;
- оценка тестов;
- тестирование;
- оценка анализа уязвимостей.

Нередко проводятся выборочные проверки, когда вместо всего (относительно однородного) множества свидетельств анализируется представительное подмножество, что позволяет сэкономить ресурсы при сохранении необходимого уровня доверия безопасности. Размер выборки должен быть обоснован математически и экономически, но при анализе реализации объекта оценки он должен составлять не менее 20 %.

Ошибки, обнаруженные при выборочной проверке, подразделяются на систематические и случайные. После исправления систематической ошибки необходимо произвести новую выборку; после случайной этого не требуется.

Допускается выборочная проверка доказательств, тестов, результатов анализа скрытых каналов, выполнения требований к содержанию и представлению свидетельств, выборочное тестирование.

В остальных ситуациях такой способ можно применять только в исключительных случаях, когда полная проверка требует слишком больших ресурсов по сравнению с другими действиями в процессе оценки или когда она не существенно увеличивает доверие безопасности. При этом необходимо обосновать допустимость и целесообразность выборочного подхода.

В «Общей методологии» специально подчеркивается, что сами по себе большие размеры и высокая сложность ОО не оправдывают замены полных

проверок выборочными, поскольку для оценки безопасности подобных объектов заведомо требуется много сил и средств.

Необходимый элемент оценки – проверка *внутренней согласованности* каждого из представленных свидетельств, а также внешней взаимной согласованности различных свидетельств.

Внутренняя согласованность проверяется в первую очередь для сущностей, имеющих несколько представлений: для спецификаций и проектов всех уровней, а также для руководств.

Проверка *внешней согласованности* производится для описаний функций, параметров безопасности, процедур и событий, связанных с безопасностью, поскольку эти описания могут содержаться в разных документах.

Внутренняя несогласованность высокоуровневых сущностей может иметь глобальные последствия для процесса оценки. Например, выявление противоречий в целях заставляет заново проанализировать требования и функции безопасности.

Разные подзадачи в процессе оценки могут выполняться в произвольном порядке или параллельно, однако существуют зависимости, накладывающие некоторые ограничения на очередность выполнения. Наиболее очевидное из них состоит в том, что анализ ЗБ *должен выполняться до* каких бы то ни было проверок ОО.

Задание по безопасности среди других характеристик ОО определяет его границы и спектр рассматриваемых угроз. Следовательно, процесс и результат оценки одного и того же продукта в сочетании с разными заданиями могут быть разными. Например, если в продукте содержатся средства межсетевого экранирования и поддержки виртуальных частных сетей (ВЧС), но в ЗБ предусмотрена исключительно защита внутренней сети от внешних угроз, то свойства ВЧС-функций важны лишь в контексте возможности обхода средств экранирования. Даже если ВЧС-функции не обеспечивают конфиденциальности сетевых потоков данных, продукт с таким заданием получит положительную оценку.

Заметим, что набор проверяемых требований необходим при сертификации не только по «Общим критериям». Нередко производитель в рекламных целях ограничивается кратким «продукт сертифицирован», что по сути бессодержательно и может ввести в заблуждение потребителя, так как зачастую означает соответствие каким-либо условиям общего характера (например отсутствуют недекларированные возможности).

Важным моментом, обычно вызывающим много вопросов, является *анализ уязвимостей* и *стойкости* функций безопасности.

Цель обоих видов проверки заключается в выявлении степени устойчивости ОО по отношению к атакам, выполняемым нарушителем с определенным (низким, умеренным или высоким) *потенциалом нападения*.

Анализ уязвимостей применяется ко всем функциям безопасности; при этом не делается каких-либо предположений относительно корректности их реализации, сохранения целостности, возможности обхода и т. п.

Анализу стойкости подвергаются только функции безопасности, реализованные с помощью вероятностных или перестановочных механизмов, у которых и проверяется стойкость – базовая, средняя или высокая (базовая означает защищенность от нарушителя с низким *потенциалом нападения*). В принципе все вероятностные функции можно считать уязвимыми, а подобный анализ классифицировать как анализ уязвимостей специального вида.

Для успешного нападения необходимо сначала идентифицировать, а затем использовать некоторую уязвимость. Оба действия оцениваются с точки зрения временных затрат, необходимой квалификации, уровня знаний об ОО, характера и продолжительности доступа к ОО, необходимых аппаратно-программных и иных ресурсов.

Перечисленные составляющие не являются независимыми. Высокая квалификация может сэкономить время, а специальное оборудование – упростить и ускорить доступ к ОО. Следовательно, если оценивать каждый параметр количественно, то результирующую функцию, характеризующую серьезность уязвимости, естественно сделать аддитивной.

В табл. 2.1 – 2.5 содержатся условные баллы, присваиваемые параметрам уязвимости в зависимости от того, в какой диапазон или на какой уровень они попадают. Для получения *общего рейтинга* нужно выбрать по одному значению из обоих числовых столбцов всех таблиц и сложить эти десять чисел. При оценке *стойкости функций безопасности* фаза идентификации не рассматривается (предполагается, что уязвимость известна), поэтому достаточно выбрать и сложить пять чисел из последних столбцов.

Таблица 2.1

Оценка уязвимости в зависимости от времени ее идентификации и использования

Диапазон	Идентификация уязвимости, усл. балл.	Использование уязвимости, усл. балл.
< 0,5 часа	0	0
< суток	2	3
< месяца	3	5
> месяца	5	8

Если уязвимость можно идентифицировать и/или использовать несколькими способами, для каждого из них вычисляется рейтинг и из полученных значений выбирается минимальное, т. е. уязвимость характеризуется самым простым методом успешного нападения.

Таблица 2.2

Оценка уязвимости в зависимости от уровня квалификации, необходимого для ее идентификации и использования

Уровень	Идентификация уязвимости, усл. балл.	Использование уязвимости, усл. балл.
Любитель	0	0
Специалист	2	2
Эксперт	5	4

Таблица 2.3

Оценка уязвимости в зависимости от уровня знаний об объекте оценки, необходимого для ее идентификации и использования

Уровень	Идентификация уязвимости, усл. балл.	Использование уязвимости, усл. балл.
Отсутствие знаний	0	0
Общедоступные знания	2	2
Конфиденциальные сведения	5	4

Таблица 2.4

Оценка уязвимости в зависимости от времени доступа к объекту оценки, требуемого для ее идентификации и использования

Диапазон	Идентификация уязвимости, усл. балл.	Использование уязвимости, усл. балл.
< 0,5 часа или доступ незаметен	0	0
< суток	2	4
< месяца	3	6
> месяца	4	9

Таблица 2.5

Оценка уязвимости в зависимости от аппаратно-программных и иных ресурсов (оборудования), необходимых для ее идентификации и использования

Уровень	Идентификация уязвимости, усл. балл.	Использование уязвимости, усл. балл.
Отсутствие оборудования	0	0
Стандартное оборудование	1	2
Специальное оборудование	3	4
Заказное оборудование	5	6

В табл. 2.6 и 2.7 приведены диапазоны рейтинга, которые характеризуют стойкость функции безопасности и потенциал нападения соответственно.

Согласно «Общей методологии» *потенциал нападения* оценивается в общем и целом по той же схеме, что и степень риска от наличия уязвимостей, с некоторыми очевидными отличиями (например, из нескольких сценариев нападения выбирается худший, с наибольшим потенциалом). Считается, что он является функцией уровня мотивации злоумышленника, его квалификации и имеющихся ресурсов. Мотивация влияет на выделяемое на атаки время и, возможно, на привлекаемые ресурсы и подбор нападающих.

Таблица 2.6

Диапазоны рейтинга, характеризующие стойкость функции безопасности

Диапазон	Стойкость функции безопасности
10 – 17	Базовая
18 – 24	Средняя
> 24	Высокая

Таблица 2.7

Диапазоны рейтинга, характеризующие потенциал нападения

Диапазон	Потенциал нападения
< 10	Низкий
10 – 17	Умеренный
18 – 24	Высокий
> 24	Нереально высокий

Нападение может быть успешным, только если его потенциал *не меньше* рейтинга уязвимости. Отсюда следует, в частности, что уязвимости с рейтингом выше 24 устойчивы к нападению с высоким потенциалом, поэтому их практическое использование злоумышленниками представляется нереальным.

Отметим, что потенциал предполагаемых нападений на ОО выявляется дважды: при анализе ЗБ для выбора надлежащих мер противодействия и при анализе уязвимостей для определения достаточности выбранных мер и качества их реализации.

Рассмотрим пример анализа стойкости функции безопасности. Пусть доступ к информационной системе осуществляется посредством территориально разнесенных терминалов, работа за которыми не контролируется. Авторизованные пользователи проходят аутентификацию путем введения паролей, состоящих из четырех различных цифр. Если пароль введен неверно, терминал блокируется на одну минуту. Требуется оценить стойкость такой парольной защиты для заданного пользователя с известным нападающему входным именем. Для нападения выбран один терминал, временем ввода можно пренебречь.

Очевидно, число возможных парольных последовательностей составляет $10 \cdot 9 \cdot 8 \cdot 7 = 5040$.

Для успешного подбора пароля методом полного перебора требуется примерно 2520 попыток, которые можно произвести за 42 ч, что больше суток, но меньше месяца. Никакой квалификации, знаний и/или оборудования для этого не требуется. Следовательно, чтобы определить стойкость функции, достаточно сложить два числа: 5 из табл. 2.1 и 6 из табл. 2.4. Сумма 11 позволяет сделать вывод, что данная функция безопасности обладает базовой стойкостью и является устойчивой к нападению с низким потенциалом.

Наконец, рассмотрим последнюю, *выходную задачу*. Ее цель – сформулировать замечания и получить *технический отчет оценки*.

Текст с замечаниями не является обязательным. Он необходим, если в процессе оценки выявились какие-либо неясности или проблемы.

Технический отчет оценки – это главный выходной документ, от качества которого во многом зависит повторяемость и воспроизводимость результатов оценки, т. е. возможность их многократного использования. «Общая методология» предписывает следующую структуру подобных отчетов:

- введение;
- архитектурное (высокоуровневое) описание ОО с рассмотрением основных компонентов;
- описание процесса оценки, примененных методов, методологий, инструментальных средств и стандартов;
- представление результатов оценки;
- выводы и рекомендации;
- список представленных свидетельств;
- список сокращений, словарь терминов;
- список замечаний.

Знание «Общей методологии» необходимо оценщикам и разработчикам.

2.4. Контрольные вопросы

1. Что собой представляет стандарт «Общие критерии оценки безопасности информационных технологий»?

2. Какие стандарты в сфере безопасности информационных технологий приняты в Республике Беларусь?

3. Укажите основные свойства общих критериев безопасности.

4. Что такое «объект оценки» в «среде безопасности»?

5. Поясните смысл определений «класс», «семейство», «компонент», «элемент».

6. Какие вы знаете виды требований безопасности?

7. Поясните основные идеи «Общей методологии оценки безопасности информационных технологий», разработанной на основе стандарта «Общие критерии».

3. «Общие критерии». Функциональные требования безопасности

3.1. Концепция представления функциональных требований

Функциональные требования безопасности, приведенные во второй части «ОК», являются базовым набором для формирования профилей защиты или ЗБ. Они направлены на противодействие угрозам в предполагаемой среде функционирования объекта и/или на реализацию провозглашаемой организационной ПБ и выдвигаемых предположений.

Часть вторая «Общих критериев» предназначена для использования заказчиками (потребителями), разработчиками и экспертами безопасных продуктов или систем ИТ.

Заказчики могут использовать документ для выбора необходимого профиля защиты или разработки ЗБ для реализации назначенной ПБ. Разработчики, отвечающие при проектировании объекта за реализацию предъявляемых заказчиком требований безопасности, могут найти в этой части документа стандартизированный метод уяснения сущности этих требований. Они могут также использовать содержание этой части документа как базис для последующего выбора средств безопасности объекта и механизмов реализации этих требований.

Эксперты должны использовать функциональные требования, приведенные во второй части «ОК», при проверке соответствия функциональных требований безопасности объекта, сформулированных в профиле защиты или в ЗБ, задачам безопасности ИТ, учета всех зависимостей (должно быть показано, каким образом это достигается). Кроме того, эксперты должны использовать эту часть документа при определении того, удовлетворяет ли конкретный объект заданным требованиям.

Функциональные требования безопасности, изложенные во второй части «ОК» не дают окончательного ответа на все проблемы безопасности ИТ. Вместе с тем, они предлагают набор понятных функциональных требований, которые могут быть использованы при создании защищенных продуктов или систем, отражающих потребности потребителей или рынка. Приведенные в настоящей части руководящего документа функциональные требования безопасности отражают современное состояние методологии задания требований безопасности и оценки эффективности реализации этих требований.

Вторая часть «ОК» не содержит всего возможного множества функциональных требований безопасности, а только те требования, которые, по мнению разработчиков «Общих критериев», были признаны существенными.

Ввиду того, что взгляды на проблемы ИБ и потребности заказчиков (потребителей) могут с течением времени меняться, функциональные требования, излагаемые в этой части документа, нуждаются в постоянном развитии и дополнении.

На рис. 3.1 и 3.2 показаны некоторые ключевые концепции представления функциональных требований. При объяснении сущности этих концепций используются следующие термины и их определения.

Оценка объекта связана, главным образом, с подтверждением того, что по отношению к ресурсам объекта осуществляется выбранная ПБ ОО. ПБ определяет правила, по которым объект управляет доступом к своим активам, а следовательно, ко всей информации и услугам, представляемым ОО.

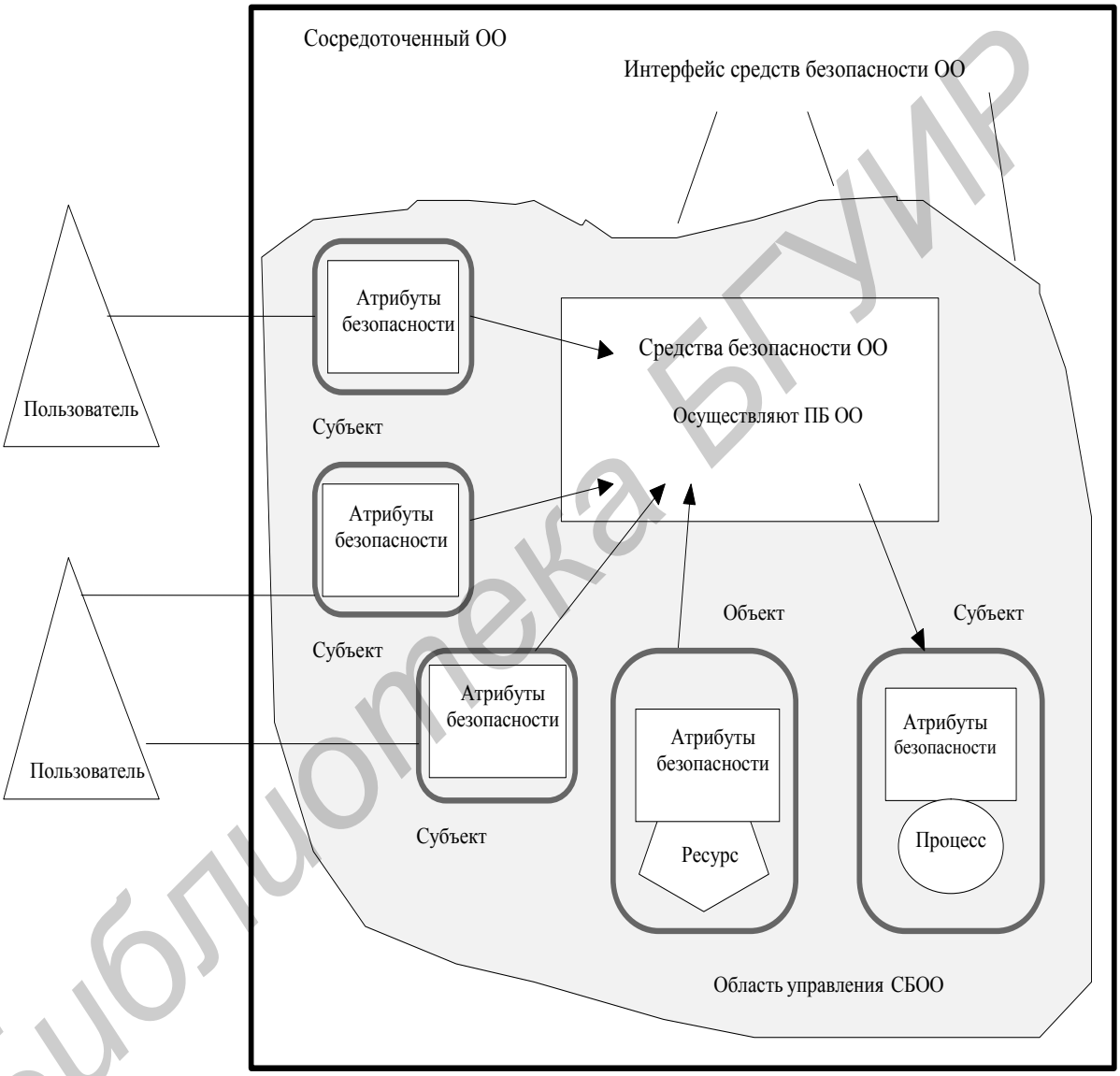

Рис. 3.1. Концепция представления функциональных требований безопасности (сосредоточенный ОО)

Политика безопасности объекта в свою очередь образуется из множества *политик функционирования средств безопасности*. Каждая политика функционирования средств безопасности имеет область управления, которая определяет субъекты, объекты и операции, управляемые этой политикой. Политика функционирования средств безопасности реализуется *средством безопасности (СБ)*.

Те части объекта, которые должны обеспечивать правильное осуществление ПБ ОО, называются *средствами безопасности объекта оценки (СБОО)*. Они состоят из совокупности аппаратного, микропрограммного и программного обеспечения объекта, которые либо непосредственно осуществляют политику безопасности объекта, либо ее дополняют.

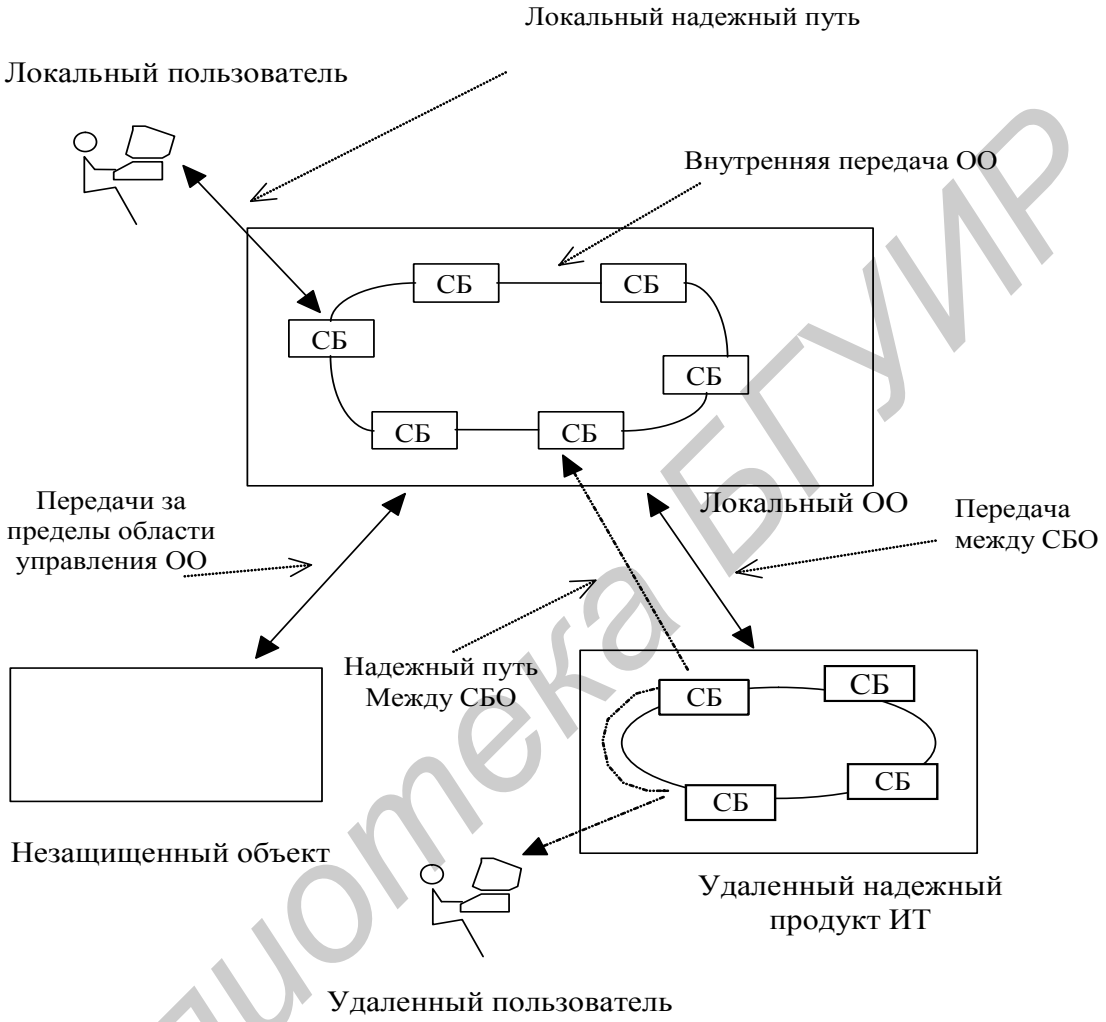

Рис. 3.2. Концепция представления функциональных требований безопасности (распределенный ОО)

Объект может быть единым изделием, содержащим аппаратное, микропрограммное и программное обеспечение.

Объект может быть также распределенным изделием, который состоит из множества физически разделенных частей. Каждая из этих частей обеспечивает часть услуг объекта и связана с другими частями через внутренний канал связи. Этот канал может быть всего лишь шиной процессора, а может являться сетью, внутренней для объекта.

Если объект состоит из нескольких частей, то каждая его часть может иметь собственное подмножество СБ, которое обменивается данными пользователя и данными СБ по внутренним каналам связи с другим подмножеством СБ.

Такая передача данных называется *внутренней передачей объекта оценки*. В этом случае отдельные подмножества СБ абстрактно образуют множество СБ, которое осуществляет ПБ объекта.

Интерфейсы объекта могут быть локальными для определенного объекта, или допускать взаимодействие с другими объектами ИТ через внешний канал связи. Эти внешние взаимодействия с другими объектами ИТ с позиции безопасности происходят в двух формах:

1) ПБ внешнего защищенного объекта ИТ и ПБ защищенного локального объекта административно скоординированы и оценены.

Обмен информацией в такой ситуации называется *передачей информации между средствами безопасности*, поскольку он происходит между СБ различных защищенных объектов;

2) внешний объект ИТ может быть не оценен с позиции безопасности (на рис. 3.2 такой объект именуется «*незащищенным объектом*»), и поэтому его СБ неизвестны.

Обмен информацией в такой ситуации называется *передачей информации за пределы области управления средств безопасности объекта оценки*, поскольку для удаленного объекта ИТ характеристики его ПБ неизвестны либо этот объект не оснащен СБ.

Множество взаимодействий, которые можно осуществлять с ОО или в пределах ОО и которые подчинены правилам ПБ ОО называется *областью управления средств безопасности*. Эта область включает определенное множество взаимодействий между субъектами, объектами и операциями в пределах объекта, но не предполагает обязательного охвата всех ресурсов объекта.

Совокупность интерфейсов, как интерактивных (человеко-машинный интерфейс) так и программных (интерфейс программных приложений), через которые может быть получен доступ к ресурсам средств безопасности, либо через которые может быть получена информация от средств безопасности, называется *интерфейсом средств безопасности объекта оценки*.

Этот интерфейс определяет возможности средств безопасности по проведению политики безопасности объекта оценки.

Пользователи не включаются в состав объекта и поэтому не находятся в пределах области управления СБ. Однако при использовании предоставляемых объектом услуг они взаимодействуют с объектом через интерфейс СБ.

В данном документе выделены два типа пользователей: пользователи – лица и пользователи – внешние объекты ИТ. Среди пользователей-лиц выделены *локальные* пользователи-лица, взаимодействующие с ОО непосредственно через устройства объекта (например, через рабочие станции), и *удаленные* пользователи-лица, взаимодействующие с ОО посредством средств внешнего объекта ИТ.

Период взаимодействия пользователя и объекта называется *сеансом пользователя*. При управлении сеансом пользователя учитываются такие аспекты, как, например, аутентификация пользователя, время сеанса, метод доступа к объекту, число допустимых для пользователя одновременных сеансов.

Управление отдельными аспектами СБ (атрибутами безопасности, данными, функциями СБ) осуществляется административными действиями на основе распределения ролей. *Роль* – заранее определенное множество правил взаимодействия между пользователем и объектом.

Объект может поддерживать определение любого количества ролей. Например, роли могут быть такими: «Администратор аудита» и «Администратор учета пользователей».

Объекты содержат ресурсы, которые могут быть использованы для обработки и хранения информации. Основная задача СБ заключается в полном и корректном осуществлении ПБ объекта по отношению к ресурсам и информации, управляемым объектом.

Ресурсы объекта могут быть структурированы и использованы различными способами. В частности, в функциональных требованиях особо выделены те из них, которые позволяют обеспечить требуемые свойства безопасности. Все совокупности ресурсов, выделяемые при структурировании, могут быть охарактеризованы одним из двух способов. С одной стороны, совокупности ресурсов могут быть активными, т. е. они являются причиной действий, которые происходят в пределах объекта, и операций над информацией. Совокупности ресурсов могут быть пассивными, т. е. они являются источником или носителем информации.

Активные совокупности ресурсов называются *субъектами*. В пределах объекта могут существовать несколько типов субъектов:

а) действующие от имени авторизованного пользователя и выполняющие все правила ПБ объекта (например процессы UNIX);

б) действующие как особый функциональный процесс, который может в свою очередь действовать от имени многих пользователей (например функции в рамках архитектуры клиент/сервер);

в) действующие как часть собственно объекта (например защищенные процессы).

Функциональные требования обеспечивают реализацию ПБ объекта для перечисленных выше типов субъектов.

Пассивные совокупности ресурсов (т. е. носители информации) называются *объектами*. *Объект* – это устройство или программа в пределах области управления средств безопасности, которые хранят, передают или принимают информацию и с помощью которых субъекты выполняют операции. В случае, если субъект сам является целью операции (например при установлении связи между процессами), над субъектом можно производить действия как над объектом.

Объекты могут содержать *информацию*. Понятие «информация» введено для определения политики управления информационными потоками в соответствие с классом FDP.

Пользователи, субъекты и объекты обладают определенными *атрибутами*, которые содержат информацию, необходимую для функционирования объекта. Некоторые атрибуты, такие как имена файлов, могут иметь общее назна-

чение, в то время как другие, такие как параметры управления доступом, предназначены исключительно для проведения ПБ. Последняя группа атрибутов названа *атрибутами безопасности*. (Далее по тексту, если не оговорено особо, вместо сочетания слов «атрибут безопасности» используется слово «атрибут».)

Данные в объекте подразделяются на данные пользователя и данные СБ. На рис. 3.3 показана взаимосвязь между указанными выше данными. *Данные пользователя* – это информация, созданная пользователем или для пользователя, которая не влияет на работу СБ. Примером данных пользователя является содержимое сообщения электронной почты. *Данные средств безопасности* – это информация, созданная объектом для реализации средствами безопасности ПБ объекта. Пользователи могут влиять на данные СБ, если это предусмотрено ПБ объекта. Примерами данных СБ являются атрибуты, данные аутентификации, список управления доступом.

Два особых типа данных СБ, а именно *данные аутентификации* и *секреты*, могут (но не обязательно) совпадать. Данные аутентификации используются для проверки подлинности пользователя, запрашивающего услуги от объекта. Наиболее общая форма данных аутентификации – это *пароль*. Для эффективности этот механизм безопасности должен содержаться в секрете. В то же время не все формы данных аутентификации должны быть секретными. Устройства биометрической аутентификации (например, считыватели отпечатков пальцев, сканеры сетчатки глаз) основаны не на хранении данных в секрете, а на том, что эти данные принадлежат только одному человеку и не могут быть подделаны.

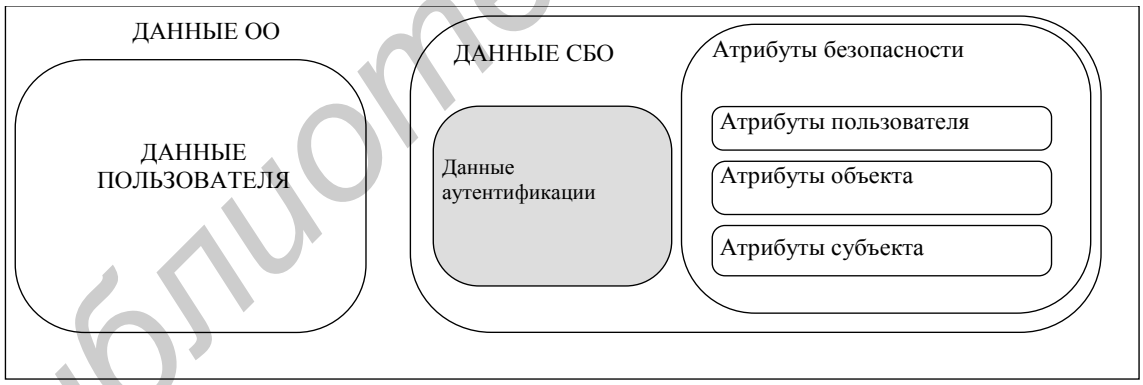

Рис. 3.3. Взаимосвязь между данными пользователя и данными средств безопасности

Термин *секрет*, используемый в функциональных требованиях в применении к данным аутентификации, может быть также применим и к другим типам данных, которые должны держаться в секрете с целью проведения специальной ПБ объекта. Например, механизм надежного канала, использующий криптографию для соблюдения конфиденциальности передаваемой по каналу информации, может быть надежным только в той степени, в какой это позволяет метод поддержки секретности криптографических ключей и предотвращения несанкционированного их раскрытия.

Не все данные аутентификации должны держаться в секрете и не все секреты используются как данные аутентификации. На рис. 3.4 показано соотношение между секретами и данными аутентификации, а также представлены типы данных, обычно встречающиеся в разделах данных аутентификации и секретов.

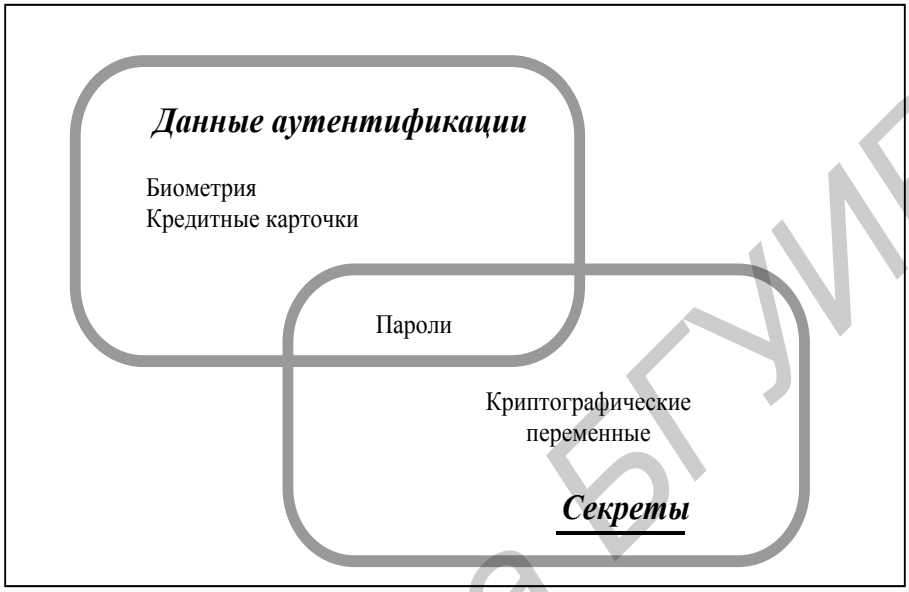

Рис. 3.4. Соотношение между данными аутентификации и секретами

3.2. Общие сведения о функциональных требованиях

3.2.1. Структура функционального класса

Функциональные требования безопасности структурно делятся на классы, семейства, компоненты и элементы. Структура функционального класса представлена на рис. 3.5.

Функциональный класс включает *имя* класса, *введение в описание* класса и *имя* одного или более функциональных *семейств*.

Имя класса содержит информацию, необходимую для идентификации функциональных классов. Каждый функциональный класс имеет уникальное полное имя и краткое имя из трех прописных букв английского алфавита, являющихся аббревиатурой имени функционального класса. Краткое имя класса используется в кратких именах семейств данного класса.

Введение в описание класса содержит краткое описание назначения класса, рисунок, описывающий имя класса, семейства данного класса и иерархию компонентов в каждом семействе.

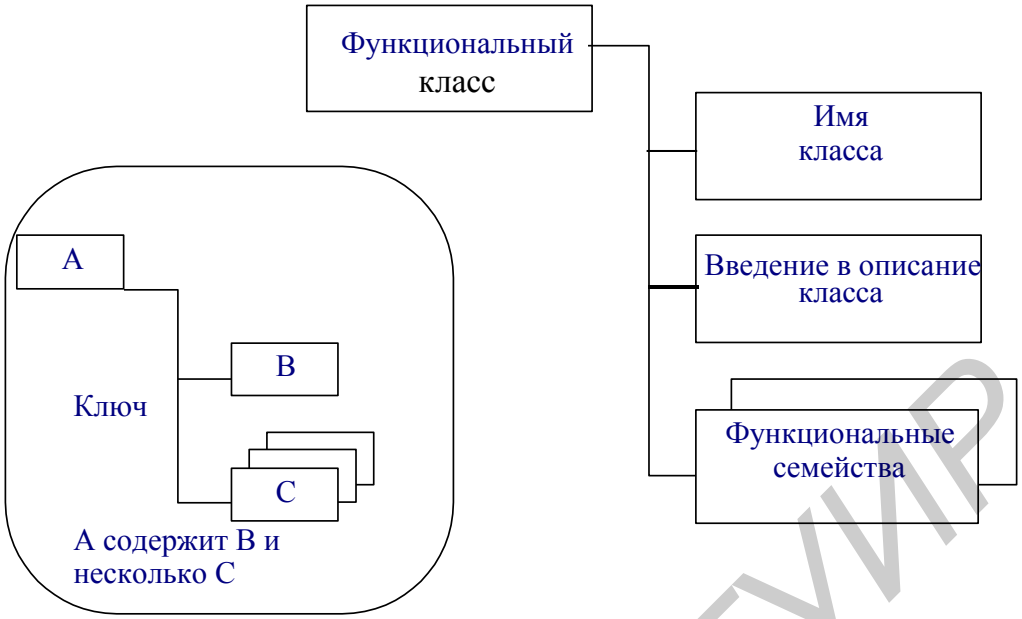

Рис. 3.5. Структура функционального класса

3.2.2. Структура функционального семейства

На рис. 3.6 представлена структура функционального семейства.

Каждое функциональное семейство имеет полное имя и краткое имя из семи символов, первые три из которых совпадают с кратким именем класса, а за ними следуют символ подчеркивания и краткое имя семейства: *XXX_YYY*.

Семейство содержит описание соответствующей ему задачи безопасности и общее описание функциональных требований, а именно:

а) *задачи безопасности* семейства описывают проблему безопасности, которая может быть решена путем реализации требований, приведенных в компонентах данного семейства;

б) в описании *функциональных требований* обобщены все требования, которые включены в компонент(ы).

Функциональные семейства содержат один или несколько компонентов, любой из которых может быть выбран для включения в профиль защиты, задание по обеспечению безопасности и в ФП. Назначение этого структурного элемента – обеспечить пользователей информацией для выбора подходящего функционального компонента, если установлено, что соответствующее семейство необходимо или полезно включить в требования безопасности объекта.

Зависимости между компонентами в пределах функционального семейства могут быть иерархическими или неиерархическими. Компонент является иерархическим (т. е. выше по уровню требований) по отношению к другому компоненту, если реализация его требований обеспечивает более высокий уровень безопасности.

Описание семейства содержит рисунок, на котором представлена иерархия компонентов в семействе.

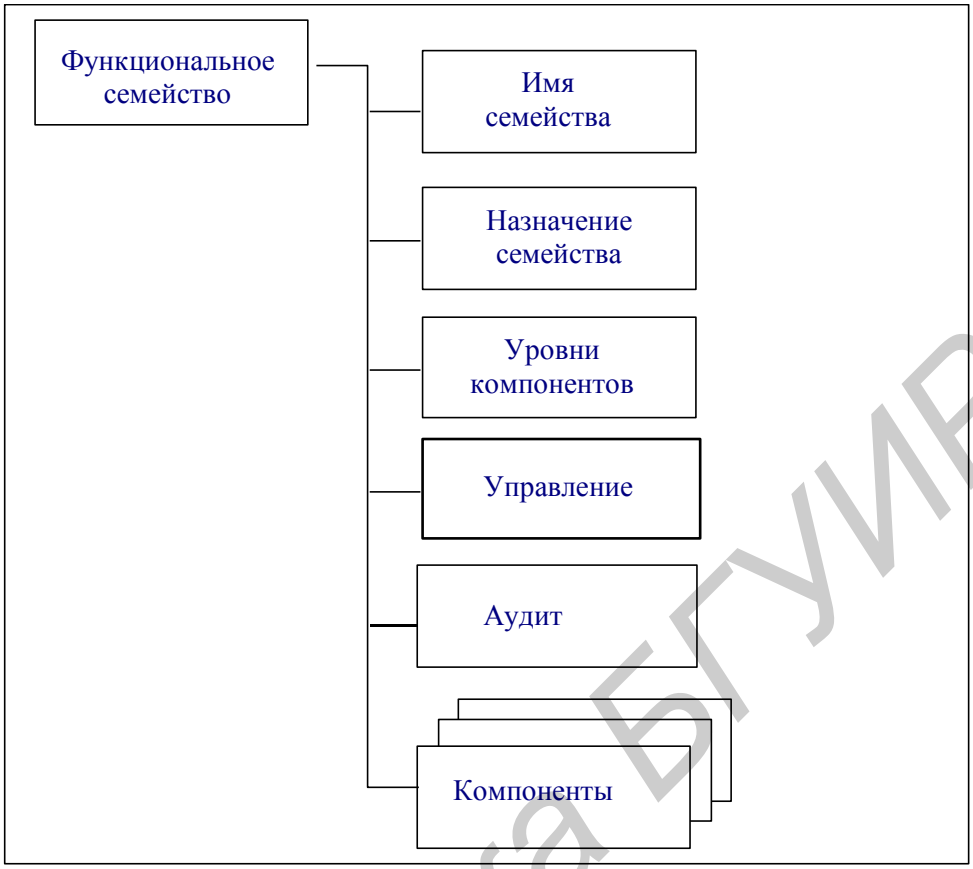

Рис. 3.6. Структура функционального семейства

Управление содержит информацию для разработчиков профилей защиты и заданий по обеспечению безопасности, касающуюся действий по управлению, которые могут быть предприняты для данного компонента.

Требования управления детализируются в компонентах класса управления FMT.

Разработчик профилей защиты и заданий по обеспечению безопасности может выбрать требования управления или при необходимости включить какие-то свои требования управления.

Аудит содержит информацию для разработчиков профилей защиты и заданий по обеспечению безопасности по выбору событий, подлежащих контролю, если требования из класса *FAU Аудит безопасности* включены в профиль защиты и в задание по обеспечению безопасности. Эти требования включают в себя связанные с безопасностью события различных уровней детализации, поддерживаемые компонентами семейства *FAU_GEN Формирование данных аудита безопасности*. Например, записи аудита могут включать в себя события следующих уровней детализации:

минимальный аудит – успешное использование механизма безопасности;

основной аудит – любое использование механизма безопасности, а также информации, касающейся используемых атрибутов безопасности;

детальный аудит – любые изменения конфигурации механизма безопасности, включая параметры конфигурации до и после изменений.

Распределение подлежащих аудиту событий по категориям является иерархическим. Например, когда описывается генерация основного аудита, то все подлежащие минимальному и основному аудитам события должны быть включены в профиль защиты и в задание по обеспечению безопасности посредством использования соответствующей операции назначения. Исключением является случай, когда событие более высокого уровня явно обеспечивает большую детализацию, чем событие более низкого уровня, и может просто заменить его. Когда описывается генерация детального аудита, то все подлежащие аудиту (минимальному, основному, детальному) события должны быть включены в профиль защиты и в задание по обеспечению безопасности.

Правила управления аудитом излагаются более подробно в классе FAU.

3.2.3. Структура функциональных компонентов операции

На рис. 3.7 представлена структура функционального компонента.

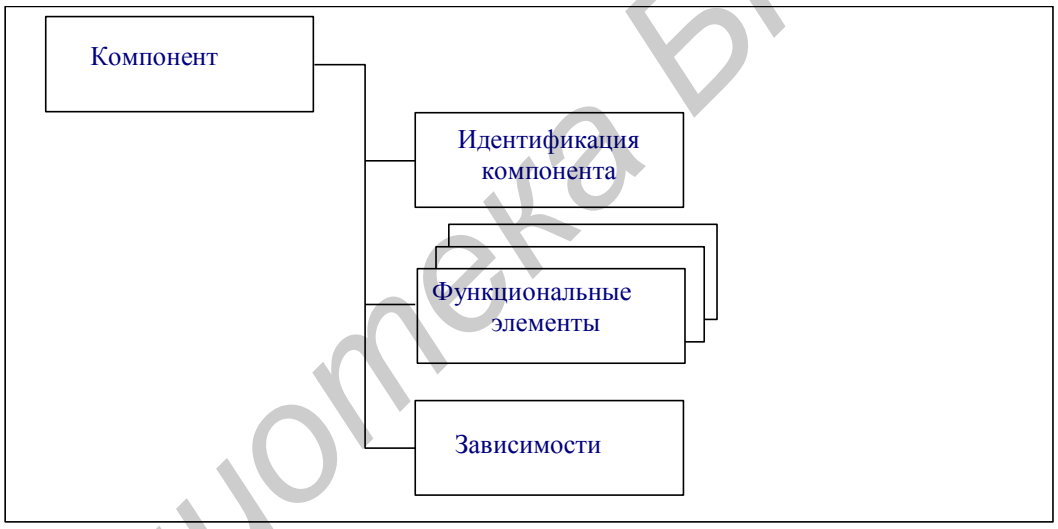

Рис. 3.7. Структура функционального компонента

Идентификация компонента содержит описательную информацию, необходимую для идентификации.

Функциональный компонент включает полное имя, краткое имя и список иерархических зависимостей.

Полное имя отражает назначение компонента.

Краткое имя отражает класс и семейство, к которым принадлежит компонент, а также номер компонента внутри семейства.

Список иерархических зависимостей – это список компонентов, по отношению к которым данный компонент является иерархическим и для которых он может использоваться для удовлетворения их зависимостей от других компонентов.

Для каждого компонента предусмотрен набор функциональных элементов. Каждый элемент определяется индивидуально и является автономным.

Функциональный элемент – это функциональное требование безопасности, дальнейшая детализация которого не дает нового содержательного результата. Он является конечным функциональным требованием безопасности, идентифицируемым и распознаваемым в настоящем документе.

В профиль защиты, в задание по обеспечению безопасности или в пакет обязательно должен включаться полный набор функциональных элементов, входящих в компонент.

Предусмотрена краткая форма имени функционального элемента. Например, имя требования FDP_IFF.4.*2* читается следующим образом: *F – функциональное требование, DP — класс Защита данных пользователя, IFF – семейство Средства управления информационными потоками, 4 – 4-й компонент Частичное исключение запрещенных информационных потоков, 2 – 2-й элемент компонента*.

Между функциональными компонентами могут существовать зависимости. Они возникают тогда, когда компонент не является автономным и нуждается в функциональных возможностях другого компонента или должен взаимодействовать с ним для обеспечения своего собственного функционирования. Зависимости могут быть прямыми, косвенными и по выбору.

Каждый функциональный компонент содержит полный список зависимостей от других функциональных и гарантийных компонентов. Некоторые компоненты могут иметь пустой список зависимостей. Зависимые компоненты могут в свою очередь являться компонентами, от которых зависят другие компоненты. Список, указываемый в компонентах, должен содержать только прямые зависимости, то есть должны быть ссылки только на те функциональные требования, которые необходимы для выполнения компонента.

Список зависимостей содержит минимум функциональных компонентов или компонентов гарантии, необходимый для удовлетворения требований безопасности, соответствующих идентифицированному компоненту. Компоненты, иерархичные идентифицируемому компоненту, также могут быть использованы для удовлетворения зависимостей.

Зависимости между функциональными компонентами, приведенные в приложении А к стандарту, являются нормативными.

Допустимые для функциональных компонентов операции

Функциональные компоненты могут выбираться непосредственно из настоящего документа либо дополняться другими требованиями в целях реализации определенных задач безопасности. Однако дополнение требований осложняется необходимостью учета зависимостей между компонентами. Это осложнение может быть разрешено, если при этом не допускать неразрешенных операций над компонентами.

Список разрешенных операций: итерация, назначение, выбор, уточнение.

Итерация применяется в тех случаях, когда необходимо охватить разные аспекты одного и того же требования (например, идентификация более чем од-

ного типа пользователя). Она позволяет несколько раз использовать один и тот же компонент в различных операциях.

Назначение позволяет определить параметр элемента в компоненте требований безопасности.

Некоторые элементы функциональных компонентов содержат параметры или переменные, которые дают возможность разработчику профиля защиты или задания по обеспечению безопасности определять политику или набор значений параметров, или переменных для включения в профиль защиты или в задание по обеспечению безопасности с целью решения определенных задач безопасности. Эти элементы четко определяют каждый параметр и ограничения на значения, которые может принимать данный параметр.

Всякий аспект элемента, допустимые значения которого могут быть однозначно описаны или перечислены, может быть представлен параметром. Параметр может быть атрибутом или правилом, сужающим требование до определенного значения или диапазона значений. Например, исходя из сформулированной задачи безопасности, элемент функционального компонента может требовать, чтобы данная операция выполнялась некоторое количество раз. В этом случае операция *назначение* будет задавать число или диапазон чисел, используемых в параметре.

Выбор – это выбор одного или нескольких элементов из перечня в компоненте с целью конкретизации области применения элемента.

Уточнение – это более детальное описание компонента.

Для всех элементов функциональных компонентов разработчик профиля защиты или задания по обеспечению безопасности имеет право ограничивать множество допустимых реализаций путем определения дополнительных деталей с целью решения задач безопасности.

Как и другие операции, уточнение не накладывает никаких совершенно новых требований. Исходя из задач безопасности, эта операция проводит по отношению к требованию, правилу, константе или условию детальную конкретизацию, интерпретацию или приписывает им специальное значение. Уточнение всего лишь еще более ограничит множество средств или механизмов, которые направлены на реализацию требований, но никогда не увеличит их перечень. Уточнение не позволяет создавать новые требования или удалять существующие и, следовательно, не увеличивает список зависимостей компонента. Разработчик профиля защиты или задания по обеспечению безопасности должен следить за тем, чтобы выполнялись необходимые зависимости для других требований, которые зависят от уточненного требования.

3.2.4. Каталог компонентов

Классы и семейства в ОК Ч.2 представлены в алфавитном порядке. В начале каждого класса есть информативная диаграмма, определяющая имя каждого класса, перечень семейств в каждом классе и перечень компонентов в каждом семействе. Диаграмма является полезной иллюстрацией иерархических отношений, которые могут существовать между компонентами.

В описании функциональных компонентов определяются зависимости между компонентом и всеми другими компонентами.

Для каждого класса приводится рисунок, описывающий иерархию семейств, аналогичную той, которая приведена на рис. 3.8.

Семейство 1 содержит три иерархических компонента, из которых компонент 2 и компонент 3 могут быть использованы для удовлетворения зависимостей компонента 1. Компонент 3 иерархичен по отношению к компоненту 2 и может также использоваться для удовлетворения зависимостей компонента 2.

Семейство 2 содержит три компонента, не все из которых иерархичны. Компоненты 1 и 2 не иерархичны никаким другим. Компонент 3 иерархичен компоненту 2 и может быть использован для удовлетворения зависимостей компонента 2, однако не может быть использован для удовлетворения зависимостей компонента 1.

Семейство 3 содержит 4 компонента. Компоненты 2, 3 и 4 иерархичны по отношению к компоненту 1. Компоненты 2 и 3 иерархичны компоненту 1, но между собой по иерархии несопоставимы. Компонент 4 иерархичен и компоненту 2, и компоненту 3.

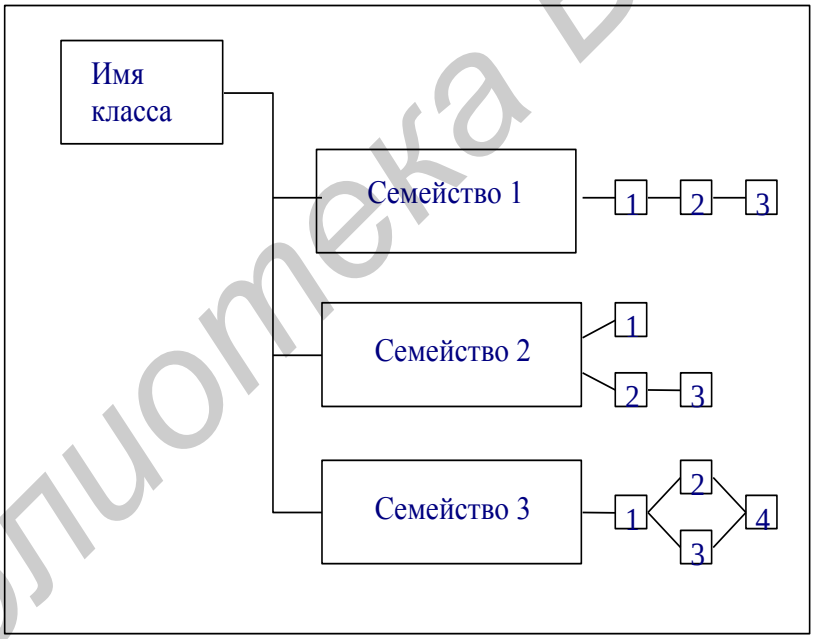

Рис. 3.8. Пример информативной диаграммы структуры класса

При описании взаимосвязи между компонентами внутри семейства используется соглашение о *применении жирного шрифта*. В соответствии с этим соглашением все новые требования выделяются жирным шрифтом. Иерархиче

ские компоненты, требования и/или зависимости выделяются жирным шрифтом в тех случаях, когда они расширены или изменены так, что превышают требования предыдущего компонента. Кроме того, жирным шрифтом выделяются все новые или расширенные разрешенные операции, не указанные в предыдущем компоненте.

3.3. Контрольные вопросы

1. Что такое функциональные требования безопасности?
2. Какова структура функционального класса и функционального семейства?
3. Поясните структуру функционального компонента. Какие операции допустимы для функциональных компонентов?

4. «Общие критерии». Требования доверия безопасности

4.1. Концепция обеспечения гарантии

Гарантийные требования формируют уверенность в том, что изделия ИТ обеспечивают достижение поставленных перед ними целей безопасности. Гарантийные требования включают совокупность требований к необходимым действиям разработчика изделия ИТ, к представлению соответствующих свидетельств обеспечения необходимой безопасности и к действиям при оценке безопасности изделия ИТ. В их состав входят следующие требования:

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

Обеспечение гарантии достигается путем оценки (активного исследования) конечного продукта или системы ИТ и документации к ним экспертами с возможно максимальным объемом и глубиной, и строгостью проводимых исследований.

Концепция обеспечения гарантии состоит в следующем:

– угрозы безопасности ИС и требования по осуществлению ПБ организации должны быть ясно сформулированы, а предложенные меры обеспечения безопасности доказуемо достаточны для решения задач безопасности;

– должны быть приняты меры по снижению вероятности наличия в системе уязвимых мест и возможностей преднамеренного использования или непреднамеренной активизации;

– должны быть приняты меры по обеспечению возможности обнаружения и ликвидации уязвимых мест, уменьшения степени проявления их признаков и для получения сведений о том, что уязвимые места использовались или активизировались.

Концепция предполагает, что могут быть нарушители, которые будут активно искать и использовать возможности нарушить ПБ в корыстных целях, активизировать уязвимости, нанося этим ущерб организации. Особенно это опасно для критически важных объектов.

Уязвимые места должны быть:

а) устранены – т. е. должны быть предприняты действия для выявления, а затем удаления или нейтрализации уязвимостей;

б) минимизированы – т. е. должны быть предприняты действия для уменьшения до допустимого остаточного уровня возможного ущерба от проявления уязвимостей;

в) отслежены – т. е. следует предпринять действия для обеспечения того, чтобы любая попытка использовать оставшиеся уязвимости была обнаружена с тем, чтобы ограничить ущерб.

Уязвимости могут возникать из-за недостатков:

а) в требованиях – т. е. изделие ИТ может обладать всеми требуемыми функциями и свойствами, но все же содержать уязвимости, которые делают его несоответствующим или неэффективным в части безопасности;

б) в проектировании – т. е. изделие ИТ не отвечает спецификации, и/или уязвимости являются следствием плохих стандартов проектирования или неправильных проектных решений;

в) в эксплуатации – т. е. изделие ИТ разработано в полном соответствии с корректными спецификациями, но уязвимости возникают как результат неадекватного управления при эксплуатации.

Таким образом, требования доверия должны охватывать все этапы жизненного цикла изделия ИТ.

4.2. Обеспечение гарантий на этапах жизненного цикла

Гарантии безопасности закладываются на этапе проектирования, реализуются на этапе производства и поддерживаются на этапе эксплуатации. Основными составляющими процесса обеспечения гарантии безопасности являются: управление конфигурацией изделия, разработка документации на изделие, оценка и сертификация безопасности, корректная поставка и ввод в эксплуатацию, поддержка доверия при эксплуатации.

4.2.1. Управление конфигурацией

Управление конфигурацией (УК) – один из методов обеспечения уверенности в правильности реализации функциональных требований и спецификаций путем установления дисциплины и управления в процессах разработки и уточнения изделия ИТ и связанной с ними информации, предотвращения несанкционированной модификации, добавления или уничтожения информации в изделии ИТ. УК направлено на то, чтобы обеспечить уверенность в целостно-

сти частей изделия ИТ, которыми оно управляет, обеспечивая прослеживание любых изменений и обеспечивая уверенность, что все изменения санкционированы.

Система УК может управлять изменениями только тех элементов, которые были помещены под УК. Элементы изделия ИТ, которые должны управляться системой управления конфигурацией, определяют область действия УК.

Она, как правило, включает:

а) представление реализации изделия ИТ;

б) всю необходимую документацию, включая проектную и тестовую, руководства администратора и пользователя, документацию УК, а также прикладные отчеты;

в) параметры конфигурации, в том числе настройки инструментальных средств разработки;

г) недостатки безопасности;

д) инструментальные средства разработки.

На начальном этапе проектирования изделия ИТ в зависимости от уровня требований доверия разрабатывается документация УК, которая включает: список элементов конфигурации изделия ИТ, план УК, методику приема элементов конфигурации под управление системы конфигурации и процедуры интеграции элементов конфигурации в состав изделия ИТ. Размещение под УК элементов изделия ИТ обеспечивает уверенность в том, что они могут быть изменены контролируемым способом с надлежащей авторизацией.

В список элементов конфигурации должны включаться: проектная документация, компоненты рабочего проекта, документация испытаний, эксплуатационная документация, документация администратора безопасности и документация системы управления конфигурацией. Для каждого элемента конфигурации изделия ИТ должно представляться его описание.

План УК должен определять порядок применения системы УК на этапах жизненного цикла изделия ИТ.

Методика приема элементов конфигурации должна описывать правила приема разработанного или измененного элемента конфигурации в составе конфигурируемой версии изделия ИТ. В методике должны быть описаны: способ идентификации элементов конфигурации, порядок контроля санкционированности производимых изменений, состав характеристик для аудита модификаций элементов конфигурации.

Процедуры интеграции должны описывать все необходимые действия, которые должны быть выполнены при включении созданного или модифицируемого элемента конфигурации в состав изделия ИТ.

В отношении недостатков безопасности должна поддерживаться информация относительно имевших место недостатков безопасности и их устранения, а также подробности относительно текущих выявленных недостатков безопасности. Возможность прослеживать недостатки безопасности при УК гарантирует то, что сообщения о недостатках безопасности не будут утрачены или забыты, а также позволяет разработчику проследить недостатки безопасности вплоть до их устранения.

Инструментальные средства разработки играют важную роль в обеспечении создания высококачественной версии изделия ИТ. Следовательно, важно управлять модификацией этих средств. Примеры средств разработки – языки программирования и компиляторы. Информация, имеющая отношение к элементам генерации версии изделия ИТ (типа опций компилятора, опций инсталляции/генерации и опций компоновки) – пример информации, относящейся к средствам разработки.

Система УК должна быть аттестована на предмет полноты охвата всех элементов конфигурации, достаточности и эффективности используемых в ней методов и средств.

Возможности управления конфигурацией определяют характеристики системы УК. Система УК должна обеспечить целостность изделия ИТ от *ранних* этапов проекта до *завершающих* этапов сопровождения. Возможности системы УК определяют уровень вероятности того, что могут произойти случайные или несанкционированные модификации элементов конфигурации.

Возможности УК должны обеспечить:

а) правильность и полноту изделия ИТ к моменту представления его потребителю;

б) контроль всех установленных элементов конфигурации в процессе разработки и оценки;

в) предотвращение несанкционированной модификации, добавления или уничтожения элементов конфигурации изделия ИТ. В основу управления конфигурацией положено требование, чтобы система УК уникально идентифицировала все элементы конфигурации. Уникальная идентификация элементов конфигурации ведет к лучшему пониманию состава изделия ИТ и позволяет выделять те его элементы, которые являются подчиненными требованиям оценки. Маркирование изделия ИТ должно обеспечить возможность различия используемых образцов. Необходимым требованием является то, что модификация элементов конфигурации должна сопровождаться назначением нового уникального идентификатора.

Система УК должна быть способна идентифицировать оригинал, используемый для создания (генерации) изделия ИТ. Это способствует сохранению целостности оригинала соответствующими техническими, физическими и процедурными мерами.

Функциональные возможности и возможности использования системы УК обеспечиваются наличием средств контроля, которые должны обеспечить целостность изделия ИТ, отсутствие в нем несанкционированных модификаций. В процессе конфигурации должны обеспечиваться учет и надлежащий анализ всех нарушений безопасности в процессе разработки, а также контроль их последующего устранения.

Повышение эффективности системы УК, особенно в тех разработках, где элементы конфигурации сложны или разрабатываются многими разработчиками, достигается применением автоматизированных систем УК. Несмотря на то, что как автоматизированные, так и ручные системы УК могут быть обойдены, игнорироваться или оказываться недостаточными, чтобы предотвратить несанкционированную модификацию, автоматизированные системы все же менее восприимчивы к человеческим ошибкам или небрежности. В частности, автоматизированные системы УК должны быть способны поддержать многочисленные изменения, которые происходят в течение разработки, и обеспечить санционирование этих изменений.

Автоматизированные средства должны обеспечивать установление различий между различными версиями изделия ИТ и определение, на какие элементы конфигурации воздействует модификация других элементов конфигурации, что помогает в определении влияния изменений на последовательные версии изделия ИТ. В свою очередь это позволит получить ценную информацию о совместимости элементов конфигурации после изменений в изделии ИТ.

4.2.2. Эксплуатационная документация

В составе эксплуатационной документации выделяются два документа, которые определяют условия безопасной эксплуатации изделия ИТ:

- руководство пользователя;
- руководство администратора.

Достаточность, полнота и понятность эксплуатационной документации являются важными факторами обеспечения правильной настройки и эффективного применения изделия ИТ.

Руководство пользователя – основное средство, доступное разработчику, для обеспечения необходимой подготовки пользователей изделия ИТ и предоставления им конкретной информации, как правильно использовать изделие

ИТ. Руководство пользователя должно содержать описание реализованных в изделии ИТ функций безопасности, руководящие принципы и инструкции по обеспечению информационной безопасности изделия ИТ.

Материалы, включаемые в руководство пользователя, должны давать возможность пользователям сформировать правильное представление о возможностях конфигурации системы безопасности (КСБ) и порядке безопасного использования его функций. Для этого руководство должно включать разъяснение двух аспектов безопасности. Во-первых, требуется объяснить, как выполняются доступные пользователю функции безопасности и как они должны быть использованы, чтобы пользователи были способны к последовательной и действенной защите своей информации. Во-вторых, требуется объяснить роль пользователя в поддержании безопасности изделия ИТ.

Руководство администратора предназначено для использования специально подготовленным персоналом, ответственным за конфигурирование, поддержание и управление изделием ИТ. Это основной документ, доступный разработчику, для обеспечения администраторов изделия ИТ детализированной и точной информацией о том, как управлять изделием ИТ безопасным способом и как эффективно использовать имеющиеся функции безопасности.

Руководство администратора должно помочь администраторам понять функции безопасности, реализованные в КСБ, включая как те функции, которые требуют, чтобы администратор выполнял обеспечивающие безопасность действия, так и те функции, которые обеспечивают безопасность критической информации. Руководство должно содержать все данные, необходимые администраторам безопасности, в том числе:

- административные функции и интерфейсы, доступные администратору;
- руководящие принципы последовательного и эффективного использования функций безопасности;
- инструкции по конфигурированию изделия ИТ и наборы параметров конфигурации;
- состав параметров КСБ, контролируемых администратором безопасности;
- предположения относительно допустимого поведения пользователей, обеспечивающие безопасное функционирование изделия ИТ;
- перечень возможных штатных и нештатных ситуаций применения изделия ИТ с описанием действий, которые должны быть при этом предприняты администратором.

Представление материалов руководств пользователя и администратора должно обеспечивать уверенность в том, что ограничения среды применения будут поняты администраторами и пользователями изделия ИТ. Противоречивое, вводящее в заблуждение, неполное или необоснованное руководство пользователя или администратора может привести их к убеждению в безопасности изделия ИТ при ее отсутствии или неполноте и может являться источником уязвимостей.

4.2.3. Поставка и ввод в эксплуатацию

Система организации поставки и ввода в эксплуатацию изделия ИТ должна определять требования к мерам, процедурам и стандартам, применяемым к безопасной поставке, установке и вводе в эксплуатацию для сохранения безопасности изделия ИТ.

Организация поставки должна охватывать процедуры поддержки безопасности в течение передачи изделия ИТ пользователю как при первоначальной поставке, так и при последующих модификациях. Организация должна предусматривать специальные меры и процедуры, требуемые для подтверждения подлинности передаваемого изделия ИТ, исключения возможности преднамеренного и непреднамеренного внесений изменений в актуальную версию, замену ее фальсифицированной версией при доставке изделия ИТ от организации разработчика до объекта пользователя.

Процедуры установки, генерации и запуска должны предусматривать меры и процедуры контроля правильности формирования эксплуатационной версии изделия ИТ, настройки всех необходимых параметров КСБ и запуска изделия ИТ безопасным способом, как это предписано разработчиком. Они должны предусматривать безопасный переход от нахождения представления реализации изделия ИТ под управлением конфигурации к начальным операциям в эксплуатационной среде пользователя. Описание процедур установки, генерации и запуска должно обеспечить знание администратором параметров конфигурации изделия ИТ и того, как они могут повлиять на КСБ.

Содержание процедур установки, генерации и запуска находится в зависимости от различных аспектов, например: является ли изделие ИТ продуктом или системой; поставляется ли изделие ИТ в готовом к эксплуатации состоянии или оно должно устанавливаться владельцем и т. д. Для конкретного изделия ИТ обычно будет иметься разделение ответственности по установке, генерации и запуску между разработчиком и владельцем изделия ИТ, но имеются примеры, где все действия производятся одной стороной. Например, для смарт-карты все аспекты установки, генерации и запуска могут выполняться разработчиком.

С другой стороны, изделие ИТ может быть поставлено в форме программного обеспечения, где все аспекты установки, генерации и запуска выполняются владельцем по месту пользования.

Процедуры установки, генерации и запуска могут либо содержаться в отдельном документе, либо быть включены разделом в другую эксплуатационную документацию.

4.2.4. Поддержка доверия при эксплуатации

Поддержка доверия к безопасности изделия ИТ при эксплуатации направлена на сохранение уровня доверия к его безопасности, т. е. на обеспечение соответствия изделия ИТ его ЗБ при изменениях в изделии ИТ или в среде его применения. В число таких важных для безопасности изменений входит обнаружение новых угроз или уязвимостей безопасности, изменения в требованиях пользователя, исправление недостатков, найденных в сертифицированном изделии ИТ, а также другие модификации его функциональных возможностей.

Одним из способов обеспечения поддержки доверия является переоценка изделия ИТ. Термин «переоценка» здесь означает оценку новой версии изделия ИТ, учитывающую все изменения, произведенные в сертифицированной ранее версии изделия ИТ, при которой по возможности используются результаты предыдущего оценивания.

Во многих случаях внесения изменений вряд ли будет практично выполнять переоценку каждой новой версии изделия ИТ для продолжения поддержки доверия. Однако. в некоторых случаях изменения могут быть настолько значительны, что для продолжения поддержки доверия обязательна только полная переоценка.

Чтобы обеспечить продолжение поддержки доверия к безопасности изделия ИТ без обязательного требования формальной переоценки, разработчик должен представить свидетельство, показывающее, что изделие ИТ продолжает удовлетворять ЗБ (например свидетельство разработчика о тестировании).

При описании процесса поддержки изделия ИТ используются два понятия в отношении его версий:

а) сертифицированная версия изделия ИТ – версия, которая была оценена и сертифицирована;

б) актуальная (текущая) версия изделия ИТ – версия, которая отличается в некотором отношении от сертифицированной версии; это может быть, например:

- новый выпуск изделия ИТ;

• сертифицированная версия с уточнениями, внесенными для исправления вновь обнаруженных ошибок;

• та же самая базовая версия изделия ИТ, но на аппаратной или программной платформе, отличной от прежней. Цикл поддержки доверия подразделяется на три следующие фазы:

а) фаза приемки изделия ИТ для поддержки;

б) фаза мониторинга;

в) фаза переоценки.

Цикл поддержки доверия проиллюстрирован на рис. 4.1.

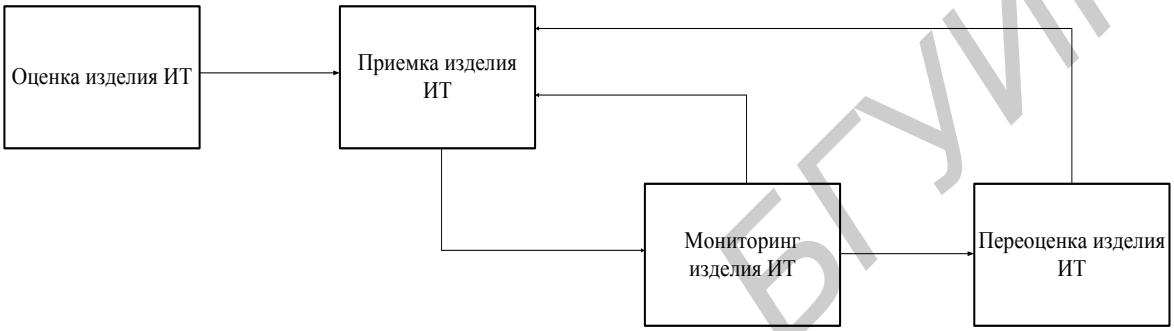

Рис. 4.1. Пример цикла поддержки доверия

В фазе мониторинга невозможно повысить уровень доверия к безопасности изделия ИТ, это может быть достигнуто только посредством новой оценки безопасности.

Приемка изделия ИТ для поддержки

В первой фазе цикла поддержки доверия разработчик принимает план поддержки доверия (ПД), а также представляет отчет о категорировании компонентов изделия ИТ, которые затем независимо проверяются оценщиком.

План ПД определяет этапы и процедуры, которые разработчик должен выполнить, чтобы обеспечить поддержание уровня доверия к безопасности, который был установлен для оцененного изделия ИТ, после изменений, внесенных в изделие ИТ или произошедших в среде его применения. План ПД охватывает один цикл поддержки доверия.

Процесс внесения изменений в изделие ИТ, который находится на поддержке, не может продолжаться бесконечно долго: в какой-то момент времени переоценка безопасности становится неизбежной. Момент принятия решения о начале переоценки зависит от накопившихся изменений и в особенности от их значимости. При этом большое количество малых изменений может иметь воздействие на доверие к безопасности, эквивалентное действию значительного

изменения. Смысл понятия «значительное изменение» будет зависеть от типа изделия ИТ и от содержания его задания по безопасности.

План ПД должен устанавливать предел для изменений в изделии ИТ, которые могут быть сделаны в фазе мониторинга. Конкретный подход к установлению предела подчинен общему замыслу поддержки доверия к безопасности изделия ИТ. При этом предполагается, что к переоценке могут приводить следующие типы изменений:

а) значительное изменение задания по безопасности (т. е. значительные изменения среды безопасности, целей безопасности или функциональных требований безопасности, а также любое повышение требований доверия);

б) значительное изменение внешних интерфейсов КСБ, категорированных как осуществляющие ПБ изделия ИТ;

в) значительное изменение подсистем КСБ, категорированных как осуществляющие ПБ изделия ИТ. Необходимо отметить, что на подход к контролю изменений, сделанных во время поддержки, могут повлиять любые механизмы, предусмотренные в изделии ИТ для автоматизированного мониторинга безопасности сертифицированной конфигурации. Такие механизмы могут предотвращать недопустимые или повреждающие изменения при попытке внести их в эксплуатируемое изделие ИТ.

В плане ПД требуется определить процедуры, используемые для поддержки доверия в течение цикла поддержки доверия. Предусматриваются четыре типа процедур:

1) процедуры управления конфигурацией, контролирующие и регистрирующие изменения в изделии ИТ;

2) процедуры для поддержки «свидетельства доверия», ключевой аспект которых – функциональное тестирование изделия ИТ;

3) процедуры анализа влияния на безопасность изменений, которым подвергается изделие ИТ, и сопровождения отчета о категорировании компонентов изделия ИТ после внесения изменений;

4) процедуры устранения недостатков, включая отслеживание и исправление выявленных недостатков безопасности. План ПД, как ожидается, должен оставаться применимым до завершения цикла поддержки доверия (т. е. завершения планируемой переоценки), после которого потребуется составить новый план ПД. План ПД будет признан недействительным, если разработчик не придерживается этого плана или вносит в изделие ИТ изменения, находящиеся за рамками плана ПД. Обновленный план ПД должен быть заново представлен на рассмотрение и принят прежде, чем изделие ИТ войдет в новую фазу мониторинга.

В дополнение к плану ПД при приемке изделия ИТ для поддержки разрабатывается также отчет о категорировании компонентов изделия ИТ.

Отчет о категорировании компонентов представляет произведенное категорирование компонентов изделия ИТ (например подсистем КСБ) согласно их важности для безопасности. Это категорирование применяется разработчиком при поддержке изделия ИТ как основа для анализа воздействий на безопасность, а также для последующей его переоценки.

Рис. 4.2. Пример подхода к приемке изделия ИТ для поддержки

Отчет о категорировании компонентов изделия ИТ охватывает все представления КСБ на поддерживаемом уровне доверия. Отчет о категорировании должен также идентифицировать:

а) любые аппаратные, программно-аппаратные и программные компоненты, которые являются внешними по отношению к изделию ИТ и удовлетворяют требованиям безопасности ИТ, определенным в ЗБ;

б) любые инструментальные средства разработки, изменение которых будет влиять на требуемую уверенность в том, что изделие ИТ удовлетворяет ЗБ.

Отчет о категорировании компонентов должен содержать описание подхода, используемого для категорирования компонентов изделия ИТ. Как минимум, требуется, чтобы компоненты были разделены на осуществляющие и не осуществляющие ПБ изделия ИТ.

В свою очередь компоненты, осуществляющие ПБ, могут быть категорированы на критичные для безопасности и на поддерживающие безопасность, в частности:

а) критичные для безопасности компоненты изделия ИТ – те, которые непосредственно ответственны за осуществление хотя бы одной функции безопасности, определенной в ЗБ;

б) поддерживающие безопасность компоненты изделия ИТ – те, которые неявно ответственны за осуществление какой-либо функции безопасности (и поэтому некритичны для безопасности), но которые, тем не менее, участвуют в поддержке КСБ. Последний класс может быть далее разделен на два различных типа компонентов:

• те, которые косвенно обеспечивают выполнение критичных для безопасности компонентов изделия ИТ и для которых, следовательно, обязательно правильное функционирование;

• те, которые никак не обеспечивают такое выполнение, но для которых, тем не менее, должна существовать уверенность, что они не ведут себя опасным способом (т.е. не активизируют уязвимости безопасности).

Описание схемы категорирования предназначено для выбора категории, к которой должен быть отнесен любой новый компонент изделия ИТ, а также, когда потребуется, для изменения категории существующего компонента после изменений в изделии ИТ или его ЗБ.

Начальное категорирование компонентов основывается на свидетельстве, представленном разработчиком при проведении оценки изделия ИТ и прошедшем независимую экспертизу.

Мониторинг изделия ИТ

В фазе мониторинга в одной или нескольких контрольных точках цикла разработчик проводит анализ влияния на безопасность и выдает заключение о результатах поддержки доверия к безопасности изделия ИТ в соответствии с установленными планами и процедурами. От разработчика требуется подтверждение следования принятым планам и процедурам и правильности выполнения анализа влияния на безопасность.

Анализ влияния на безопасность должен доказать эффективность поддержки доверия путем его проведения разработчиком при всех изменениях, выполняемых в сертифицированном ранее изделии ИТ.

Анализ влияния на безопасность, проводимый разработчиком, основывается на отчете о категорировании компонентов; изменения в компонентах, осуществляющих политику безопасности, могут повлиять на уверенность в том, что изделие ИТ продолжает отвечать ЗБ после внесения изменений. Поэтому все такие изменения требуют анализа их влияния на безопасность, чтобы показать, что они не угрожают безопасности изделия ИТ.

Анализ влияния на безопасность идентифицирует изменения в сертифицированной версии изделия ИТ в терминах компонентов, которые или являются новыми, или изменились. При экспертизе проверяется точность этой информации или в течение фазы мониторинга, или при переоценке изделия ИТ.

Процедуры устранения недостатков должны обеспечить, чтобы недостатки, обнаруженные потребителями изделия ИТ, были прослежены и исправлены во время его сопровождения разработчиком. При оценке изделия ИТ необходимо оценить политику и процедуры, которые разработчик установил для выявления и устранения недостатков и распространения информации об обнаруженном недостатке и его исправлении.

Процедуры устранения недостатков должны описать методы для реагирования на все типы недостатков, с которыми можно столкнуться в процессе сопровождения. Некоторые недостатки не могут быть исправлены немедленно. Возможны и такие случаи, когда недостаток не может быть исправлен и должны применяться другие (например организационные) меры. Представленная документация должна охватывать процедуры для обеспечения исправлений в местах эксплуатации, а также для обеспечения безопасности информации о недостатках, для которых исправления отложены, включая меры обеспечения безопасности на время отсрочки, или для которых исправления вообще невозможны.

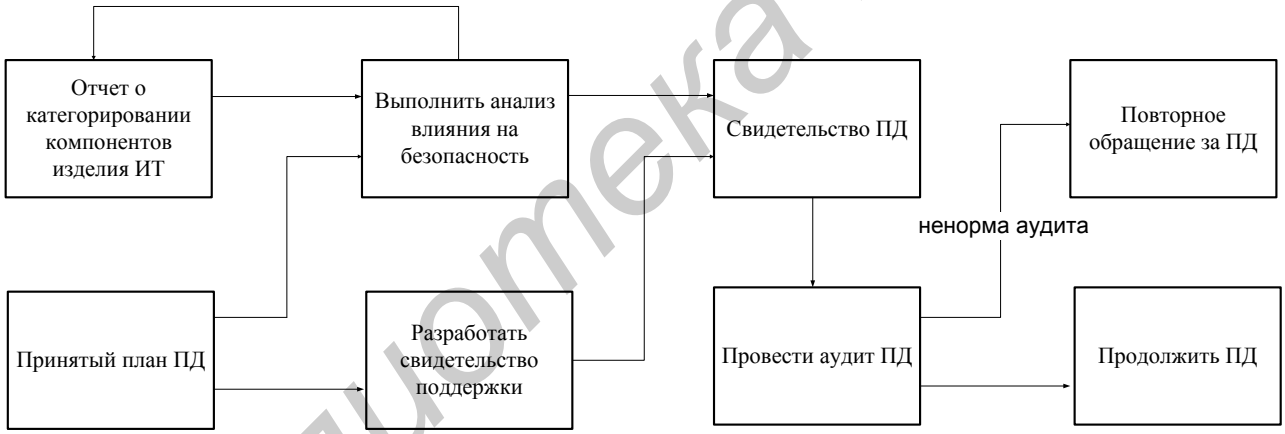

Рис. 4.3. Пример подхода к мониторингу изделия ИТ

В соответствии с графиком, определяемом в ПД, по результатам поддержки доверия разработчиком выдается заключение о текущем состоянии с выполнением плана и следовании процедурам поддержки доверия. Заключение должно включать:

а) отчеты об УК;

б) документацию, используемую при анализе влияния на безопасность, включая актуальную версию отчета о категорировании компонентов изделия ИТ и свидетельства для соответствующих требований доверия, такие как модификации проекта, тестовая документация, новые версии руководств и т. д.;

в) свидетельство отслеживания недостатков безопасности.

Заключение по результатам поддержки безопасности подвергается независимой экспертизе.

Переоценка

Третья фаза цикла поддержки – фаза переоценки, завершающая цикл, в которой актуальная версия изделия ИТ представляется на рассмотрение для переоценки, основанной на изменениях, которым подверглась сертифицированная версия.

Действия переоценки могут устанавливаться в плане ПД или могут потребоваться в ответ на непредвиденные значительные изменения в изделии ИТ или его среде, после которых продолжение поддержки доверия рассматривается как недопустимое.

4.3. Контрольные вопросы

1. Что такое гарантийные требования обеспечения безопасности?
2. Поясните, как осуществляется управление конфигурацией изделия ИТ?
3. Какая документация должна определять условия безопасной эксплуатации изделия ИТ?
4. Как осуществляется поддержка доверия при эксплуатации изделия ИТ?

5. Профиль защиты и задание по безопасности

5.1. Общие сведения о форме задания требований безопасности

Профиль защиты (ПЗ) представляет собой независимый от реализации типовой набор требований безопасности для совокупности изделий определенного вида, отвечающий соответствующим целям безопасности. ПЗ предназначен для многократного использования и определяет требования безопасности изделий ИТ, включая функциональные требования и требования доверия, в отношении которых установлено, что они являются достаточными и эффективными для достижения установленных целей безопасности.

ПЗ разрабатываются и используются как стандартизованные наборы требований с целью повышения обоснованности задания требований безопасности изделий ИТ, оценки безопасности и возможности проведения сравнительного анализа уровня безопасности различных изделий ИТ.

ЗБ содержит совокупность требований безопасности для конкретного изделия ИТ, которые обеспечивают достижение установленных целей безопасности. ЗБ представляет собой набор требований безопасности, которые могут быть определены ссылкой на профили защиты, ссылкой на отдельные стандартизованные требования или же содержать требования в явном виде.

ЗБ формируется разработчиком изделия ИТ и является основой для проведения оценки и сертификации изделия ИТ.

Пакет представляет собой промежуточный набор компонентов требований безопасности, которые удовлетворяют определенному подмножеству целей безопасности. Пакет предназначен для неоднократного использования и содержит требования, для которых установлено, что они являются пригодными и эффективными для достижения определенных целей. Пакет может использоваться в структуре больших пакетов, профилей защиты и ЗБ.

Итак, «ОК» обеспечивают охват основных классов и учет особенностей изделий ИТ при задании требований безопасности.

В «ОК» отсутствует жесткая шкала классификации изделий ИТ по уровню безопасности. Вместо этого вводится понятие ПЗ – стандартизованного набора требований, предназначенного для многократного использования, и ЗБ для конкретного изделия ИТ.

«ОК» регламентируют структуру и основное содержание профилей защиты и ЗБ.

5.2. Структура и содержание профиля защиты

В табл. 5.1 приведена определенная в «ОК» структура ПЗ. Из указанных в ней разделов ПЗ только раздел «Замечания по применению» не является обязательным и может содержать дополнительную информацию, которая полезна при создании, оценке и использовании ОО.

Таблица 5.1

Структура профиля защиты

Название раздела
1. ВВЕДЕНИЕ ПЗ
1.1. Идентификация ПЗ
1.2. Аннотация ПЗ
2. ОПИСАНИЕ ОО
3. СРЕДА БЕЗОПАСНОСТИ ОО
3.1. Предположения безопасности
3.2. Угрозы
3.3. Политика безопасности организации
4. ЦЕЛИ БЕЗОПАСНОСТИ
4.1. Цели безопасности для ОО
4.2. Цели безопасности для среды
5. ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИТ
5.1. Функциональные требования безопасности ОО
5.2. Требования доверия к безопасности ОО
5.3. Требования безопасности для среды ИТ
6. ЗАМЕЧАНИЯ ПО ПРИМЕНЕНИЮ
7. ОБОСНОВАНИЕ
7.1. Логическое обоснование целей безопасности
7.2. Логическое обоснование требований безопасности

5.2.1. Введение ПЗ

Введение ПЗ должно содержать информацию управления документооборотом и обзорную информацию, необходимые для работы с реестром ПЗ:

а) идентификация ПЗ должна обеспечить маркировку и описательную информацию, необходимую для идентификации, каталогизации, регистрации ПЗ и ссылок на него;

б) аннотация ПЗ содержит общую характеристику ПЗ в описательной форме. Аннотация должна быть достаточно подробной, чтобы потенциальный пользователь ПЗ мог решить, представляет ли ПЗ для него интерес. Аннотация должна быть также применима для размещения в виде самостоятельного реферата в каталогах и реестрах ПЗ.

5.2.2. Описание объекта оценки

В этой части ПЗ должно содержаться описание ОО, служащее цели лучшего понимания требований безопасности и дающее представление о типе ОО и его общих характеристиках.

Если ОО представляет собой изделие ИТ, основной функцией которого является безопасность, то раздел «Описание объекта оценки» может использоваться для более подробного описания условий применения, в которых предполагается использовать ОО.

5.2.3. Среда безопасности объекта оценки (предположения безопасности, угрозы, политика безопасности организации)

Раздел ПЗ «Среда безопасности ОО» должен содержать описание аспектов безопасности среды, в которой будет использоваться ОО, и предполагаемый способ его применения. Это описание должно включать описание предположений безопасности, угроз и ПБ организации.

Описание предположений безопасности должно содержать описание аспектов безопасности среды, в которой предполагается использовать ОО. Описание предположений безопасности должно включать:

• информацию относительно предполагаемого использования ОО, в том числе такие аспекты, как предполагаемая область применения, потенциальная значимость активов и возможные ограничения использования;

• информацию относительно среды применения ОО, в том числе аспекты физического окружения, персонала и внешних связей.

Описание угроз должно включать все те угрозы активам, от которых требуется защита средствами ОО или его среды. Заметим, что могут быть приведены не все существующие в среде угрозы, а только те, которые влияют на безопасную эксплуатацию ОО.

При описании угрозы должны быть указаны: идентифицированный источник угрозы (нарушитель), способ нападения и активы, подверженные нападению. Для источника угрозы следует рассмотреть компетентность, доступные ресурсы и мотивацию. Для нападения следует указать: возможность нападения, методы нападения и используемые уязвимости.

Описание ПБ организации. Каждое положение ПБ организации необходимо представлять в виде, позволяющем установить четкие цели безопасности.

Для физически распределенного ОО аспекты среды безопасности (предположения безопасности, угрозы, ПБ организации) следует рассматривать отдельно для каждой части ОО.

5.2.4. Цели безопасности

Цели безопасности должны учитывать все предположения безопасности, ПБ организации и отражать заявленное намерение противостоять всем выявленным угрозам. Различаются следующие категории целей безопасности: цели безопасности для ОО и цели безопасности для среды ОО.

Необходимо отметить, что цели безопасности для среды могут повторять полностью или частично, некоторые из предположений сделанные при описании среды безопасности ОО.

Если противостояние угрозе или проведение ПБ частично возлагается на ОО, а частично на его среду, соответствующая цель безопасности формулируется как для ОО, так и для его среды.

5.2.5. Требования безопасности ИТ

В этом разделе ПЗ подробно определяются требования безопасности ИТ, которые должны выполняться ОО или его средой.

В описании требований безопасности ОО определяются функциональные требования и требования доверия, которым должен удовлетворять ОО, а также приводимые свидетельства его оценки для достижения целей безопасности. Требования безопасности ОО должны формироваться следующим образом:

1. Функциональные требования к ОО должны определяться, где это возможно, на основе функциональных компонентов из «ОК».

Если требования доверия к ОО включают компонент «Оценка стойкости функции безопасности ОО» (например, уровень гарантии оценки (УГО) 2 и выше), то при изложении функциональных требований ОО должен устанавливаться минимальный уровень стойкости для функций безопасности, реализованных с помощью вероятностного или перестановочного механизмов.

Как составная часть оценки стойкости функций безопасности ОО должен быть оценен уровень стойкости, установленный посредством возможного задания метрики для отдельных функций безопасности ОО, и минимальный уровень стойкости для ОО в целом.

2. Гарантийные требования безопасности ОО перечислены в третьей части «ОК», хотя возможно применение требований доверия и не из «ОК».

Выбор гарантийных требований требует учета следующих факторов:

• ценность активов, подлежащих защите, и осознанный риск компрометации этих активов;

• техническая реализуемость;

• вероятная стоимость разработки и оценки;

• затраты времени, необходимые для разработки и оценки ОО;

• осознанные рыночные требования (в случае коммерческих продуктов);

• любые идентифицированные зависимости между функциональными компонентами и компонентами доверия. Чем больше ценность (важность) активов, подлежащих защите, чем выше риск компрометации этих активов, тем выше должны быть требования доверия, предъявляемые к изделию ИТ.

Другие факторы, такие как стоимость и затраты времени, действуют как ограничения на практически достижимый уровень доверия. Выбор гарантийных требований к безопасности относительно не сложен, когда он заключается в выборе соответствующего оценочного уровня доверия, из числа определенных в ОК.

Выбор гарантийных требований к безопасности (ГТБ) также упрощается при наличии других применимых пакетов гарантийных требований.

В некоторых случаях, когда УГО уже выбран, может потребоваться включить в ПЗ или ЗБ дополнительные гарантийные требования. Выбор таких компонентов целесообразен для усиления требований по отдельным аспектам, например, для более тщательного анализа уязвимостей с особым вниманием к тестированию возможностей проникновения в систему.

В случае включения дополнительных гарантийных требований автор ПЗ должен обеспечить удовлетворение новых зависимостей. Например, если ПЗ усиливает УГО 3 компонентом «Высокостойкий», то в данный УГО следует также включить компоненты «Описательный проект нижнего уровня» и «Подмножество реализации функций безопасности объекта», поскольку они отсутствуют в УГО 3.

Расширение УГО в ПЗ может также осуществляться за счет включения дополнительных компонентов доверия, не входящих в «ОК».

Помимо описания требований безопасности ОО в данном разделе ПЗ может приводиться необязательное описание требований безопасности для среды ИТ. Отметим, что требования безопасности среды, не относящиеся к ИТ, которые часто бывают полезны на практике, могут формально не являться частью ПЗ, поскольку они не связаны непосредственно с реализацией ОО.

Перечисленные ниже общие условия в равной степени относятся как к функциональным, так и к гарантийным требованиям как для ОО, так и для его среды ИТ:

1. Когда это возможно, все требования безопасности ИТ следует вводить ссылкой на компоненты требований из частей 2 и 3 «ОК». Дополнительные требования могут быть сформулированы явным образом, без ссылки на «ОК».

2. Все явно сформулированные функциональные требования и требования доверия должны быть изложены четко и однозначно, чтобы не возникало трудностей с их оценкой и демонстрацией соответствия. Уровень детализации и способ выражения функциональных требований и требований доверия, принятый в ОК, должен использоваться как образец.

3. Если выбраны компоненты требований, в которых определены разрешенные операции (назначение, выбор), то эти операции должны использоваться в ПЗ для конкретизации требований до уровня детализации, необходимого для демонстрации выполнения целей безопасности. Все разрешенные операции, которые не исполнены в ПЗ, должны быть отмечены как незавершенные (для последующего завершения в ЗБ).

4. Используя при описании требований безопасности ОО разрешенные операции над компонентами требований, можно, где это необходимо, устанавливать или запрещать применение определенных механизмов безопасности.

5. Следует удовлетворить все зависимости между требованиями безопасности. Все случаи неудовлетворения зависимостей должны быть строго обоснованы.

5.2.6. Обоснование

В этом разделе ПЗ представляется свидетельство, используемое при оценке ПЗ. Это свидетельство призвано подтвердить, что ПЗ является полной и взаимосвязанной совокупностью требований и соответствующий ему ОО обеспечит эффективный набор мер безопасности ИТ в определенной среде безопасности. Раздел должен включать следующее:

а) логическое обоснование целей безопасности, которое демонстрирует, что сформулированные цели охватывают все идентифицированные аспекты безопасности в рассматриваемой среде ИТ и верно отражают их;

б) логическое обоснование требований безопасности, которое демонстрирует, что совокупность требований безопасности (ОО и его среды) соответствует целям безопасности и обеспечивает их достижение. Необходимо показать следующее:

1) комбинация отдельных компонентов функциональных требований и

гарантийных требований для ОО и его среды ИТ в совокупности отвечает изложенным целям безопасности;

2) набор требований безопасности образует единое, внутренне непротиворечивое целое;

3) выбор требований безопасности строго обоснован. Специальное обоснование необходимо:

• для выбора требований, не содержащихся в частях 2 и 3 «ОК»;

• для выбора требований доверия, не включенных в УГО;

• для случаев неудовлетворения зависимостей.

4) выбранный для ПЗ уровень стойкости функций и заявленная в явном виде стойкость функций согласуются с целями безопасности для ОО.

5.3. Структура и содержание задания по безопасности

ЗБ по структуре во многом похоже на ПЗ и содержит дополнительную информацию, разъясняющую, каким образом требования ПЗ должны быть реализованы для конкретного изделия ИТ. В задании по безопасности имеется следующая информация, отсутствующая в ПЗ:

1) во введение дополнительно включены материалы о соответствии ОК (соответствие или расширение части 2 ОК; соответствие, уточнение или расширение части 3 ОК, привлечение ПЗ);

2) новый раздел «Краткая спецификация ОО» представляет функции безопасности и меры доверия для конкретного изделия ИТ;

3) новый раздел «Утверждения о соответствии ПЗ» показывает, каким ПЗ должно соответствовать ЗБ, если такое соответствие предполагается;

4) раздел ЗБ «Обоснование» дополнительно содержит свидетельство, подтверждающее, что краткая спецификация ОО отвечает требованиям безопасности, приведенным в ЗБ, и что все утверждения о соответствии ПЗ справедливы. ЗБ представляет собой основу для соглашения между разработчиками, оценщиками и потребителями о характеристиках безопасности ОО и области применения оценки.

В табл. 5.2 приведена определенная в ОК структура ЗБ.

Ниже приведено более подробное описание содержания дополнительных (по сравнению с ПЗ) разделов ЗБ и существенно расширенного раздела «Обоснование».

Краткая спецификация ОО

Краткая спецификация ОО предназначена для конкретизации представления требований безопасности ОО. Она должна предоставить описание функций

безопасности и мер доверия к ОО, которые отвечают требованиям безопасности ОО. Следует отметить, что информация о функциях безопасности, являющаяся частью краткой спецификации ОО, в некоторых случаях может быть идентична информации, предоставляемой частью требований семейства ADV_FSP.

Таблица 5.2

Структура задания по безопасности

Наименование раздела
1.1. ВВЕДЕНИЕ ЗБ 1.2. Идентификация ЗБ 1.3. Аннотация ЗБ 1.4. Соответствие ОК
2. ОПИСАНИЕ ОО
3. СРЕДА БЕЗОПАСНОСТИ ОО 3.1. Предположения безопасности 3.2. Угрозы 3.3. Политика безопасности организации
4. ЦЕЛИ БЕЗОПАСНОСТИ 4.1. Цели безопасности для ОО 4.2. Цели безопасности для среды
5. ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИТ 5.1. Функциональные требования безопасности ОО 5.2. Требования доверия к безопасности ОО 5.3. Требования безопасности для среды ИТ
6. КРАТКАЯ СПЕЦИФИКАЦИЯ ОО 6.1. Функции безопасности ОО 6.2. Меры доверия
7. ТРЕБОВАНИЯ СООТВЕТСТВИЯ ПЗ 7.1. Ссылка на ПЗ 7.2. Конкретизация ПЗ 7.3. Дополнение ПЗ
8. ОБОСНОВАНИЕ 8.1. Логическое обоснование целей безопасности 8.2. Логическое обоснование требований безопасности 8.3. Логическое обоснование краткой спецификации ОО 8.4. Логическое обоснование утверждений о соответствии ПЗ

Краткая спецификация ОО включает следующее:

а) изложение функций безопасности ОО, которое должно охватить все функции безопасности и определить, каким образом эти функции удовлетворяют функциональным требованиям. Изложение должно содержать двунаправленное сопоставление функций и требований с четким указанием, какие функции каким требованиям удовлетворяют и что удовлетворены все требования. Каждая функция безопасности должна участвовать в удовлетворении по меньшей мере одного функционального требования безопасности ОО:

1) функции безопасности ИТ должны быть определены неформальным образом на уровне детализации, необходимом для понимания их назначения;

2) все ссылки на механизмы безопасности должны быть сопоставлены с соответствующими функциями так, чтобы было видно, какие механизмы используются при реализации каждой функции;

3) если в состав требований доверия к ОО включен компонент AVA_SOF.l, то должны быть идентифицированы все функции безопасности ИТ, реализованные с помощью вероятностного или перестановочного механизмов. Возможность нарушения механизмов таких функций посредством преднамеренного или случайного воздействия имеет непосредственное отношение к безопасности ОО. Должен быть проведен анализ стойкости всех этих функций. Стойкость каждой идентифицированной функции должна быть определена и заявлена либо как базовая, средняя или высокая, либо с применением дополнительно введенной метрики стойкости. Свидетельство, приводимое в отношении стойкости функции безопасности, должно быть достаточным, чтобы позволить оценщикам сделать независимую оценку и подтвердить, что утверждения о стойкости адекватны и корректны;

б) изложение гарантийных требований, которое должно специфицировать меры доверия к безопасности ОО, заявленные для удовлетворения изложенных гарантийных требований. Гарантийные требования должны быть сопоставлены с требованиями таким образом, чтобы было понятно, какие меры в удовлетворении каких требований участвуют.

Там, где это возможно, гарантийные требования следует определить путем ссылки на соответствующие планы обеспечения качества, жизненного цикла или управления.

Утверждения о соответствии ПЗ

В ЗБ могут содержаться утверждения, что ОО соответствует требованиям одного или нескольких ПЗ. Влияние на ЗБ такого утверждения может быть сведено к одному из следующих вариантов:

1) если в ЗБ утверждается только соответствие требованиям какого-либо

ПЗ без необходимости их дальнейшего уточнения, то ссылки на ПЗ достаточно, чтобы определить и строго обосновать цели и требования безопасности ОО;

2) если в ЗБ утверждается соответствие требованиям какого-либо ПЗ, а требования этого ПЗ нуждаются в дальнейшем уточнении, то в ЗБ это уточнение должны быть выполнено. Такая ситуация обычно возникает, если ПЗ содержит незавершенные операции. В некоторых случаях, когда завершение операций приводит к существенным изменениям, может оказаться предпочтительным для ясности повторно изложить содержание ПЗ в составе ЗБ;

3) если в ЗБ утверждается соответствие требованиям какого-либо ПЗ, но при этом последний расширяется путем добавления дополнительных целей и требований, то в ЗБ должны быть определены эти дополнения с учетом того, что ссылки на ПЗ может быть достаточно для определения целей и требований безопасности. В некоторых случаях, когда дополнения к ПЗ существенны, может оказаться предпочтительным для ясности повторно изложить содержание ПЗ в составе ЗБ;

4) случай, когда в ЗБ утверждается частичное соответствие ПЗ, не приемлем для оценки в рамках ОК.

Если сделано утверждение о соответствии какому-либо ПЗ, то изложение утверждений о соответствии должно содержать следующий материал для каждого ПЗ:

1) ссылку на ПЗ плюс любые дополнительные материалы, которые могут потребоваться в соответствии с этим утверждением;

2) конкретизацию ПЗ, идентифицирующую те требования безопасности ИТ, в которых выполняются операции, разрешенные в ПЗ, или дополнительно уточняются требования ПЗ;

3) дополнение ПЗ, идентифицирующее цели и требования безопасности ОО, которые дополняют цели и требования ПЗ.

Обоснование ЗБ

В этом разделе должно быть представлено свидетельство, используемое при оценке ЗБ. Это свидетельство призвано подтвердить, что ЗБ является полной, непротиворечивой совокупностью требований, что соответствующий ему ОО обеспечит эффективный набор мер безопасности ИТ в определенной среде безопасности, а краткая спецификация ОО согласуется с требованиями.

Обоснование также демонстрирует, что все утверждения о соответствии ПЗ верны. Раздел должен включать следующее:

а) логическое обоснование целей безопасности, которое демонстрирует, что сформулированные цели охватывают все аспекты безопасности в рассматриваемой среде ИТ и верно отражают их;

б) логическое обоснование требований безопасности, которое демонстрирует, что совокупность требований безопасности (ОО и его среды) соответствует целям безопасности и обеспечивает их достижение. Необходимо показать следующее:

1) комбинация отдельных компонентов функциональных требований и требований доверия для ОО и его среды ИТ обеспечивает достижение установленных целей безопасности;

2) набор требований безопасности образует единое, внутренне непротиворечивое целое;

3) выбор требований безопасности обоснован. Специальное обоснование обеспечивает:

• выбор требований, не содержащихся в частях 2 и 3 «ОК»;

• выбор требований доверия, не включенных в какой-либо УГО;

• случаи неудовлетворения зависимостей;

4) выбранный для ЗБ уровень стойкости функций и заявленная в явном виде стойкость согласуются с целями безопасности;

в) логическое обоснование краткой спецификация ОО, показывающее, что функции безопасности и меры доверия ОО отвечают требованиям безопасности. Должно быть продемонстрировано следующее:

1) сочетание специфицированных для ОО функций безопасности при совместном использовании удовлетворяет функциональным требованиям безопасности;

2) справедливы сделанные утверждения о стойкости функций безопасности или заявление, что в таких утверждениях нет необходимости;

3) обосновано утверждение, что изложенные меры доверия соответствуют требованиям доверия.

Уровень детализации обоснования должен соответствовать уровню детализации определения функций безопасности.

г) логическое обоснование утверждений о соответствии ПЗ, объясняющее различия между целями и требованиями безопасности ЗБ и любого ПЗ, соответствие которому утверждается.

5.4. Примеры формулировок

5.4.1. Угрозы безопасности

T.ACCESS – уполномоченный пользователь ОО может получить доступ к информации или ресурсам без разрешения их владельца или лица, ответственного за данную информацию или данные ресурсы.

T.CONSUME – уполномоченный пользователь ОО монополизирует общие ресурсы, ставя под угрозу возможность для других уполномоченных пользователей получить доступ к этим ресурсам или использовать их.

T.COVERT – уполномоченный пользователь ОО может (преднамеренно или случайно) передавать (по скрытому каналу) закрытую информацию пользователям, которые не имеют допуска к работе с данной информацией.

T.DENY – пользователь может участвовать в передаче информации (как отправитель или получатель), а затем отрицать данный факт.

T.IMPERSON – нарушитель (постороннее лицо или сотрудник организации) может получить несанкционированный доступ к информации или ресурсам, выдавая себя за уполномоченного пользователя ОО.

T.INTEGRITY – целостность информации может быть поставлена под угрозу из-за ошибки пользователя, аппаратных ошибок или ошибок при передаче.

T.LINK – нарушитель может иметь возможность наблюдать за многократным использованием ресурсов или услуг какой-либо сущностью (субъектом или объектом) и, связывая факты такого использования, получать (выводить дедуктивным методом) информацию, которую требуется хранить в секрете.

T.MODIFY – целостность информации может быть нарушена вследствие несанкционированной модификации или разрушения информации нарушителем.

T.SECRET – пользователь ОО может (преднамеренно или случайно) наблюдать (изучать) информацию, сохраненную в ОО, к которой он не имеет допуска.

Следующие угрозы должны учитываться при формулировании целей безопасности для среды.

TE.BADMEDIA – старение и износ носителей данных или ненадлежащее хранение и обращение со сменным носителем могут привести к его порче, ведущей к потере или искажению данных, критичных по безопасности.

TE.CRASH – ошибка человека, отказ программного обеспечения, аппаратных средств или источников питания могут вызвать внезапное прерывание в работе ОО, приводящее к потере или искажению данных, критичных по безопасности.

TE.PHYSICAL – критичные по безопасности части ОО могут быть подвергнуты физической атаке, ставящей под угрозу их безопасность.

TE.PRTV1LEGE – компрометация активов ИТ может происходить в результате небрежных или преднамеренных действий, предпринятых администраторами или другими привилегированными пользователями.

TE.VIRUS – целостность и/или доступность активов ИТ может быть нарушена в результате непреднамеренного занесения в систему компьютерного вируса уполномоченным пользователем ОО.

5.4.2. Примеры политики безопасности организации

Данный пункт содержит два типичных примера ПБ организации. На практике организации могут, разумеется, иметь более детализированную политику.

ПБ организации на основе дискреционного принципа управления доступом – право доступа к конкретным объектам данных определяется на основе:

а) идентификационной информации владельца объекта;

б) идентификационной информации субъекта, осуществляющего доступ;

в) явных и неявных прав доступа к объекту, предоставленных субъекту владельцем данного объекта.

ПБ организации на основе мандатного принципа управления доступом – право доступа к информации, маркированной по степени конфиденциальности, определяется следующим образом:

а) данному лицу разрешен доступ к информации, только если оно имеет соответствующий допуск;

б) данное лицо не может понижать степень конфиденциальности информации, если у него нет на то явных полномочий.

5.4.3. Примеры предположений безопасности

Данный пункт содержит примеры предположений безопасности, относящихся к физической защите, персоналу и связности.

Примеры предположений, связанных с физической защитой

Предположение о расположении ресурсов ОО

A.LOCATE – предполагается, что ресурсы ОО расположены в пределах области действия функций управления доступом, которые предотвращают несанкционированный физический доступ.

Предположение о физической защите ОО

A.PROTECT – предполагается, что аппаратные средства и программное обеспечение ОО, критичные по безопасности, физически защищены от несанкционированной модификации потенциальными нарушителями.

Примеры предположений, связанных с персоналом

A.ADMIN – предполагается, что назначены уполномоченные администраторы, которые компетентны (т. е. обладают необходимой квалификацией),

чтобы управлять ОО и безопасностью информации. Администраторам можно доверять в том, что они не злоупотребят преднамеренно своими привилегиями для нарушения безопасности.

A.ATTACK – предполагается, что нарушители имеют высокий уровень специальных знаний и мотивации, а также располагают необходимыми ресурсами.

A.USER – предполагается, что пользователи ОО обладают необходимыми правами для доступа к информации, которой управляет ОО.

Примеры предположений, имеющих отношение к связности

A.DEVICE – предполагается, что все соединения с периферийными устройствами находятся в пределах области действия функций управления доступом.

A.FIREWALL – предполагается, что межсетевой экран настроен таким образом, что он является единственной точкой сетевого соединения между частной (приватной) сетью и потенциально враждебной сетью.

A.PEER – предполагается, что любые системы, с которыми связывается ОО, принадлежат той же организации и работают при тех же ограничениях политики безопасности.

5.4.4. Примеры целей безопасности для ОО

В данном пункте приводятся примеры целей безопасности для ОО, которые могут использоваться при формировании ПЗ или ЗБ.

O.ADMIN – ОО должен предоставить уполномоченному администратору средства, позволяющие эффективно управлять ОО и функциями безопасности, а также обеспечить, чтобы только уполномоченные администраторы могли получить доступ к таким средствам.

O.ANON – ОО должен предусматривать средства разрешения субъекту использовать ресурс или услугу без раскрытия идентификационной информации пользователя другим сущностям (объектам или субъектам).

O.AUDIT – ОО должен предусматривать средства регистрации любых событий, относящихся к безопасности, чтобы способствовать администратору в обнаружении потенциальных нарушений (атак) или неправильной настройки параметров, делающей ОО уязвимым для потенциальных нарушений (атак), оставляя пользователей подотчетными за любые связанные с безопасностью действия.

O.DAC – ОО должен предусматривать средства управления доступом отдельных пользователей или идентифицированных групп пользователей к объ-

ектам и ресурсам, по отношению к которым они являются владельцами или ответственными, в соответствии с набором правил, определенных ПБ P.DAC.

O.ENCRYPT – ОО должен предусматривать средства защиты конфиденциальности информации при передаче последней по сети.

O.ENTRY – ОО должен иметь возможность ограничения входа (доступа к ОО) пользователя на основе времени и местоположения устройства входа (доступа).

O.I&A – ОО должен выполнять уникальную идентификацию всех пользователей и аутентификацию идентификационной информации до предоставления пользователю доступа к ОО.

O.INTEGRITY – ОО должен иметь средства обнаружения нарушения целостности информации.

O.LABEL – ОО должен поддерживать метки для информации, хранимой и обрабатываемой ОО, обеспечивая их целостность. Данные, выводимые (экспортируемые) ОО, должны иметь метки конфиденциальности, в точности соответствующие внутренним меткам.

O.MAC – ОО должен защищать конфиденциальность информации, находящейся под управлением ОО, в соответствии с ПБ P.MAC.

O.PROTECT – ОО должен иметь средства собственной защиты от внешнего вмешательства или вмешательства со стороны недоверенных субъектов или от попыток недоверенных субъектов обойти функции безопасности ОО.

5.4.5. Примеры целей безопасности для среды

В данном пункте приводятся примеры целей безопасности для среды, которые могут использоваться при формировании ПЗ/ЗБ.

OE.AUDITLOG – администраторы ОО должны обеспечить эффективное использование функциональных возможностей аудита. В частности:

а) должны быть приняты меры для обеспечения непрерывного ведения журналов аудита, например, путем регулярного архивирования файлов регистрационных журналов с тем, чтобы предоставить требуемое свободное пространство;

б) журналы аудита следует регулярно проверять и принимать меры по обнаружению нарушений безопасности или событий, которые свидетельствуют о возможности таких нарушений в будущем.

OE.AUTHDATA – ответственные за ОО должны обеспечить, чтобы данные аутентификации для каждой учетной записи пользователя ОО сохранялись в тайне и не раскрывались лицам, не уполномоченным использовать данную учетную запись.

OE.CONNECT – ответственные за ОО должны обеспечить отсутствие подключения к внешним системам или пользователям, которые могут нарушить безопасность ИТ.

OE.INSTAJLL – ответственные за ОО должны обеспечить безопасность ОО на всех этапах его поставки, установки и эксплуатации. OE.PHYSICAL – ответственные за ОО должны обеспечить, чтобы части ОО, являющиеся критичными по безопасности, были защищены от физического нападения, которое могло бы поставить под угрозу безопасность ИТ.

5.5. Контрольные вопросы

1. Что собой представляет «профиль защиты»?
2. Какова структура и содержание «задания по безопасности»?
3. Приведите известные вам примеры формулировок угроз безопасности, политики безопасности, предположений и целей безопасности для объекта оценки и среды безопасности.

Литература

1. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель : СТБ 34.101.1-2004 (ИСО/МЭК 15408-1:1999).

2. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности : СТБ 34.101.2-2004 (ИСО/МЭК 15408-2:1999).

3. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 3. Гарантийные требования безопасности : СТБ 34.101.3-2004 (ИСО/МЭК 15408-3:1999).

4. Оценка безопасности информационных технологий / В. А. Галатенко [и др.]; под ред. В. А. Галатенко. – М. : СИП РИА, 2001.

5. Галатенко, В. А. Информационная безопасность : практический подход / В. А. Галатенко. – М. : Наука, 1998.

6. Зегжда, Д. П., Ивашко, А. М. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М. : Горячая линия – Телеком, 2000.

Учебное издание

Голиков Владимир Федорович
Черная Ирина Исааковна
Зельманский Олег Борисович

МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *Т. П. Андрейченко*
Корректор *А. В. Тюхай*
Компьютерная верстка *М. В. Гуртатовская*

Подписано в печать Формат 60x84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 3,5. Уч.-изд. л. Тираж 100 экз. Заказ 499.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6