Тема 1.1 «Оранжевая книга» (TCSEC) – общие положения

1 «Оранжевая книга» (TCSEC) – общие положения

Безопасность информационных технологий (ИТ) стоит в ряду актуальнейших проблем компьютеризации управленческой деятельности. Ее решение определяется, в первую очередь, наличием законодательных актов и нормативно-технических документов по обеспечению безопасности ИТ. Оценка безопасности информационных технологий и продуктов ИТ базируется на критериях безопасности компьютерных систем, приведенных в основополагающих документах.

В январе 1981 года в соответствии с директивой министра обороны США № 5215.1 с целью определения пригодности предлагаемых различными разработчиками компьютерных систем был создан Центр компьютерной безопасности министерства обороны США.

Позднее, в сентябре 1985 года, этот центр был переименован в Национальный центр компьютерной безопасности (National Computer Security Center; NCSC).

Оценивание компьютерных систем осуществлялось и осуществляется на основании стандарта, известного как Критерии оценки пригодности компьютерных систем министерства обороны (Department of Defence Trusted Computer System Evaluation Criteria; TCSEC), установленного в 1983 году директивой министра обороны N5200.28-STD. TCSEC известен также под названием «Оранжевая книга» по цвету обложки книги. TCSEC определяет средства, которые должны быть включены в компьютерную систему для того, чтобы такая система была безопасной в отношении обработки критической информации.

Требования TCSEC, предъявляемые к компьютерной системе (продукту) в процессе оценивания, условно можно разделить на четыре типа – требования проведения последовательной политики безопасности (security policy), требования ведения учета использования продукта (accounts), требования доверия к продукту (assurance) и требования к документации на продукт.

Согласно TCSEC, для оценивания компьютерных систем выделено четыре основных группы безопасности, которые в свою очередь делятся на классы безопасности:

1) Группа Д – Minimal Protection (минимальная защита) – объединяет компьютерные системы, не удовлетворяющие требованиям безопасности высших классов. В данном случае группа и класс совпадают.

2) Группа С – Discretionary Protection (избирательная защита) – объединяет системы, обеспечивающие набор средств защиты, применяемых пользователем, включая средства общего контроля и учета субъектов и их действий. Эта группа имеет два класса:

– класс С1 – Discretionary Security Protection (избирательная защита безопасности) – объединяет системы с разделением пользователей и данных;

– класс С2 – Controlled Access Protection (защита контролируемого доступа) – объединяет системы, обеспечивающие более тонкие средства защиты по сравнению с системами класса С1, делающие пользователей индивидуально различимыми в их действиях посредством процедур контроля входа и контроля за событиями, затрагивающими безопасность системы и изоляцию данных.

Примечание: Компьютерные системы, которые могут быть использованы для нужд министерства обороны США, должны как минимум иметь рейтинг безопасности С2.

1) группа В – Mandatory Protection (полномочная защита) – имеет три класса:

– класс В1 – Labeled Security Protection (меточная защита безопасности) – объединяет системы, удовлетворяющие всем требованиям класса С2, дополнительно реализующие заранее определенную модель безопасности, поддерживающие метки субъектов и объектов, полный контроль доступа. Вся выдаваемая информация регистрируется, все выявленные при тестировании недостатки должны быть устранены;

– класс В2 – Structured Protection (структурированная защита) – объединяет системы, в которых реализована четко определенная и задокументированная

формализованная модель обеспечения безопасности, а меточный механизм разделения и контроля доступа, реализованный в системах класса B1, распространен на всех пользователей, все данные и все виды доступа. По сравнению с классом B1 ужесточены требования по идентификации пользователей, контролю за исполнением команд управления, усилена поддержка администратора и операторов системы. Должны быть проанализированы и перекрыты все возможности обхода защиты. Системы класса B2 считаются «относительно неуязвимыми» для несанкционированного доступа;

– класс B3 – Security Domains (области безопасности) – объединяет системы, имеющие специальные комплексы безопасности. В системах этого класса должен быть механизм регистрации всех видов доступа любого субъекта к любому объекту. Должна быть полностью исключена возможность несанкционированного доступа. Система безопасности должна иметь небольшой объем и приемлемую сложность для того, чтобы пользователь мог в любой момент протестировать механизм безопасности. Системы этого класса должны иметь средства поддержки администратора безопасности; механизм контроля должен быть распространен вплоть до сигнализации о всех событиях, затрагивающих безопасность; должны быть средства восстановления системы. Системы этого класса считаются устойчивыми к несанкционированному доступу.

2) группа A – Verified Protection (проверяемая защита) – объединяет системы, характерные тем, что для проверки реализованных в системе средств защиты обрабатываемой или хранимой информации применяются формальные методы. Обязательным требованием является полная документированность всех аспектов проектирования, разработки и исполнения систем. Выделен единственный класс:

Раздел 1. «Оранжевая книга» (TCSEC) – оценочный стандарт информационной безопасности

Таблица 1 – Классы безопасности в «Оранжевой книге»

Требования	**К л а с с ы**					
	C1	**C2**	**B1**	**B2**	**B3**	**A1**
1 Требования к политике безопасности						
1.1 Произвольное управление доступом	+	+	=	=	+	=
1.2 Повторное использование объектов	-	+	=	=	=	=
1.3 Метки безопасности	-	-	+	+	=	=
1.4 Целостность меток безопасности	-	-	+	+	=	=
1.5 Принудительное управление доступом	-	-	+	+	=	=
2 Требования к подотчетности						
2.1 Идентификация и аутентификация	+	+	+	=	=	=
2.2 Предоставление надежного пути	-	-	-	+	+	=
2.3 Аудит	-	+	+	+	+	=
3 Требования к гарантированности						
3.1 Операционная гарантированность						
3.1.1 Архитектура системы	+	+	+	+	+	=
3.1.2 Целостность системы	+	=	=	=	=	=
3.1.3 Анализ тайных каналов передачи информации	-	-	-	+	+	+
3.1.4 Надежное администрирование	-	-	-	+	+	=
3.1.5 Надежное восстановление	-	-	-	-	+	=
3.2 Технологическая гарантированность						
3.2.1 Тестирование	+	+	+	+	+	+
3.2.2 Верификация спецификаций архитектуры	-	-	+	+	+	+
3.2.3 Конфигурационное управление	-	-	-	+	=	+
3.2.4 Надежное распространение	-	-	-	-	-	+
4 Требования к документации						
4.1 Руководство пользователя по средствам безопасности	+	=	=	=	=	=
4.2 Руководство администратора по средствам безопасности	+	+	+	+	+	+
4.2 Тестовая документация	+	=	=	+	=	+
4.4 Описание архитектуры	+	=	+	+	+	+

– класс A1 – Verified Desing (проверяемая разработка) – объединяющий системы, функционально эквивалентные системам класса B3 и не требующие каких-либо дополнительных средств. Отличительной чертой систем этого класса является анализ формальных спецификаций проекта системы и технологии исполнения, дающий в результате высокую степень гарантированности корректного исполнения системы.

Кроме этого, системы должны иметь мощные средства управления конфигурацией и средства поддержки администратора безопасности.

Основное содержание требований по классам безопасности TCSEC приведено в таблице 1.

Тема 1.2 «Оранжевая книга» (TCSEC) – основные понятия

1 Основные понятия

Оценочные стандарты выделяют важнейшие, с точки зрения ИБ, аспекты ИС, играя роль архитектурных спецификаций. Другие технические спецификации определяют, как строить ИС предписанной архитектуры.

Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем».

Данный труд, называемый чаще всего по цвету обложки «Оранжевой книгой», был впервые опубликован в августе 1983 года. Уже одно его название 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 – 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 системе, тем строже и многообразнее должна быть политика безопасности. 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 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 политики безопасности. 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 политики безопасности. Качество вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит системный администратор.

Вообще говоря, компоненты вне вычислительной базы могут не быть доверенными, однако это не должно влиять на безопасность системы в целом. В результате, для оценки доверия безопасности ИС достаточно рассмотреть только ее вычислительную базу, которая, как можно надеяться, достаточно компактна.

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.

2 Механизмы безопасности

Согласно «Оранжевой книге», политика безопасности 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 мы указывали 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. Смысл сформулированного правила понятен – 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 политику безопасности 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 делает. Средства подотчетности делятся на три категории:

- 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» рассматривается 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:

- архитектура системы;
- целостность системы;
- проверка тайных каналов передачи информации;
- доверенное администрирование;
- доверенное восстановление после сбоев.

Операционная гарантированность – это способ убедиться в том, что архитектура системы и ее реализация действительно реализуют избранную политику безопасности.

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

3 Классы безопасности

«Критерии ...» Министерства обороны США открыли путь к ранжированию информационных систем по степени доверия безопасности.

В «Оранжевой книге» определяется 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 политика безопасности и уровень гарантированности должны удовлетворять заданным требованиям, из которых мы 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 подходы к безопасности, используемые производителем, и применение этих подходов при реализации доверенной вычислительной базы.

Класс C2 (в дополнение к C1):

– 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, относящейся к доступу к объектам, контролируемым базой;

– тестирование должно подтвердить отсутствие очевидных недостатков в механизмах изоляции ресурсов и защиты регистрационной информации.

Класс B1 (в дополнение к C2):

– 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, полностью понимающих реализацию доверенной вычислительной базы, должна подвергнуть описание архитектуры, исходные и объектные коды тщательному анализу и тестированию;

– должна существовать неформальная или формальная модель политики безопасности, поддерживаемой 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 хорошо определенные, относительно независимые модули;

– системный архитектор 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 политики безопасности должна быть формальной. Для доверенной вычислительной базы должны существовать описательные спецификации верхнего уровня, точно и полно определяющие ее интерфейс;

– 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 политике безопасности системы. Администратор безопасности должен немедленно извещаться о попытках нарушения политики безопасности, а система, в случае продолжения попыток, 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 иного нарушения работы без ослабления защиты;

– должна быть продемонстрирована устойчивость доверенной вычислительной базы к попыткам проникновения.

Класс A1 (в дополнение к B3):

– 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 C – произвольное управление доступом;

– уровень B – принудительное управление доступом;

– уровень A – 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 информационной безопасности. 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.

Тема 1.3 Федеральные критерии безопасности информационных технологий

1 Общие положения

«Федеральные критерии безопасности информационных технологий» («Федеральные критерии») разрабатывались как одна из составляющих «Американского федерального стандарта по обработке информации» (Federal Information Processing Standard), призванного заменить «Оранжевую книгу».

Главной целью создания «Федеральных критериев» являлось определение универсального и открытого для дальнейшего развития набора основных требований безопасности, предъявляемых к современным информационным технологиям. Стандарт определяет обоснованный и структурированный подход к разработке требований безопасности, предъявляемых к продуктам информационных технологий с учетом областей их применения. Стандарт является обобщением основных принципов обеспечения безопасности информационных технологий, разработанных в 80-е годы, и обеспечивает преемственность по отношению к ним с целью сохранения достижений в области защиты информации.

«Федеральные критерии» содержат положения, относящиеся только к отдельным продуктам информационных технологий. Вопросы построения систем обработки информации из набора ИТ-продуктов не являются предметом рассмотрения этого документа.

2 Профиль защиты

Ключевым понятием концепции информационной безопасности «Федеральных критериев» является понятие «профиля защиты» (Protection Profile). Профиль защиты – это нормативный документ, который регламентирует все аспекты безопасности ИТ-продукта в виде требований к его проектированию, технологии разработки и квалификационному анализу. Как правило, один профиль защиты описывает несколько близких по структуре и назначению ИТ-продуктов. Основное внимание в профиле защиты уделяется требованиям к составу средств защиты и

качеству их реализации, а также их адекватности предполагаемым угрозам безопасности.

Профиль защиты состоит из следующих пяти разделов: описание, обоснование, функциональные требования к ИТ-продукту, требования к технологии разработки ИТ-продукта, требования к процессу квалификационного анализа ИТ-продукта.

Описание профиля содержит классификационную информацию, необходимую для его идентификации в специальной картотеке. «Федеральные критерии» предлагают поддерживать такую картотеку на общегосударственном уровне. Это позволит любой организации воспользоваться созданными ранее профилями защиты непосредственно или использовать их в качестве прототипов при разработке новых.

Обоснование содержит описание среды эксплуатации, предполагаемых угроз безопасности и методов использования ИТ-продукта. Кроме того, этот раздел содержит подробный перечень задач по обеспечению безопасности, решаемых с помощью данного профиля. Эта информация дает возможность определить, в какой мере данный профиль пригоден для применения в той или иной ситуации. Предполагается, что данный раздел ориентирован на службы безопасности организаций, которые изучают возможность использования ИТ-продукта, соответствующего данному профилю защиты.

3 Функциональные требования

Раздел функциональных требований к ИТ-продукту содержит описание функциональных возможностей средств защиты ИТ-продукта и определяет условия, в которых обеспечивается безопасность в виде перечня угроз, которым успешно противостоят предложенные средства защиты. Угрозы, лежащие вне этого диапазона, должны быть устранены с помощью дополнительных, не входящих в состав продукта, средств обеспечения безопасности.

Раздел требований к технологии разработки ИТ-продукта охватывает все этапы его создания, начиная от разработки проекта и заканчивая вводом готовой системы в эксплуатацию. Раздел содержит требования как к самому процессу разработки, так и к условиям, в которых она проводится, к используемым технологическим средствам, а

также к документированию этого процесса. Выполнение требований этого раздела является непременным условием для проведения квалификационного анализа и сертификации ИТ-продукта.

Раздел требований к процессу квалификационного анализа ИТ-продукта регламентирует порядок проведения квалификационного анализа в виде методики исследований и тестирования ИТ-продукта. Объем и глубина требуемых исследований зависят от наиболее вероятных типов угроз, среды применения и планируемой технологии эксплуатации.

Функциональные требования «Федеральных критериев» разделены на восемь классов и определяют все аспекты функционирования ядра безопасности (Trusted Computing Base, TCB). Под ядром безопасности понимается совокупность аппаратных, программных и специальных компонент вычислительной системы, реализующих функции защиты и обеспечения безопасности. Таксономия классов функциональных требований приведена на рисунке1.

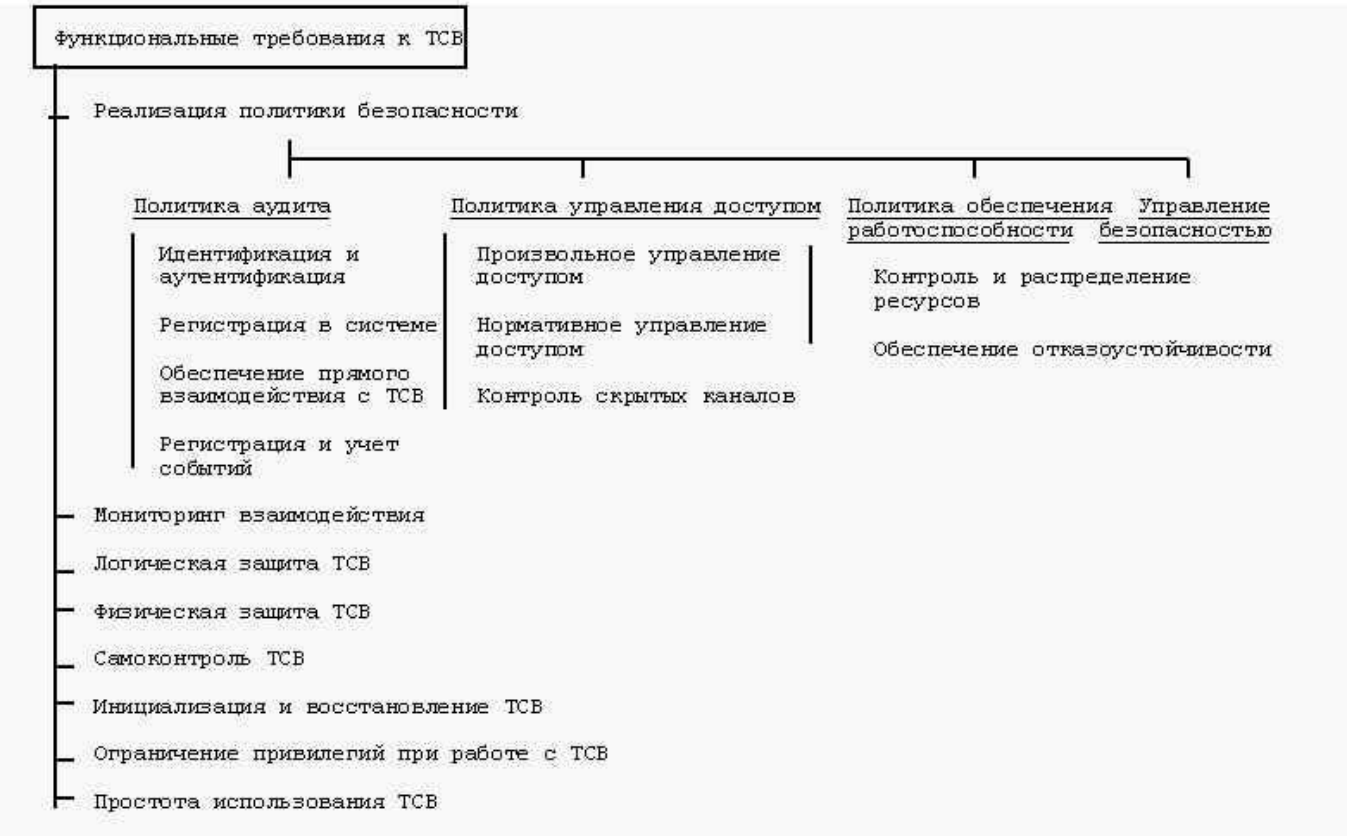

Рисунок 1 – Таксономия функциональных требований «Федеральных критериев»

Состав и содержание включенных в профиль защиты функциональных требований определяются средой эксплуатации ИТ-продукта. Чтобы обосновать выбор тех или иных требований и не вступать в противоречие с существующими стандартами в области безопасности ИТ-продуктов, функциональные требования, приведенные в «Федеральных критериях», ранжируются по уровням с помощью следующих четырех критериев: широта сферы применения, степень детализации, функциональный состав средств защиты, обеспечиваемый уровень безопасности.

Ранжирование всегда предполагает установление некоторого отношения порядка. Однако независимое ранжирование функциональных требований по каждому из приведенных критериев, хотя и дает некоторое представление о различиях между функциональными возможностями средств защиты, не позволяет установить четкую, линейную шкалу уровней безопасности. Однозначного отношения порядка, определенного на множестве функциональных требований, не существует, так как значение требований и уровень обеспечиваемой ими защиты зависят не только от их содержания, но и от назначения ИТ-продукта и среды его эксплуатации. Для одних систем наиболее важными будут идентификация и аутентификация пользователей, а для других – реализация политики управления доступом или обеспечение работоспособности.

Поэтому в «Федеральных критериях» отсутствуют рекомендации как по выбору и применению тех или иных функциональных требований, так и по определению их роли в системе обеспечения безопасности. Вместо жестких указаний этот документ содержит согласованный с предшествующими ему стандартами («Оранжевая книга», «Европейские критерии») ранжированный перечень функциональных требований и предоставляет разработчикам профиля защиты возможность самостоятельно сделать выбор необходимых методов и средств обеспечения безопасности, основанный на назначении и специфике среды эксплуатации ИТ-продукта.

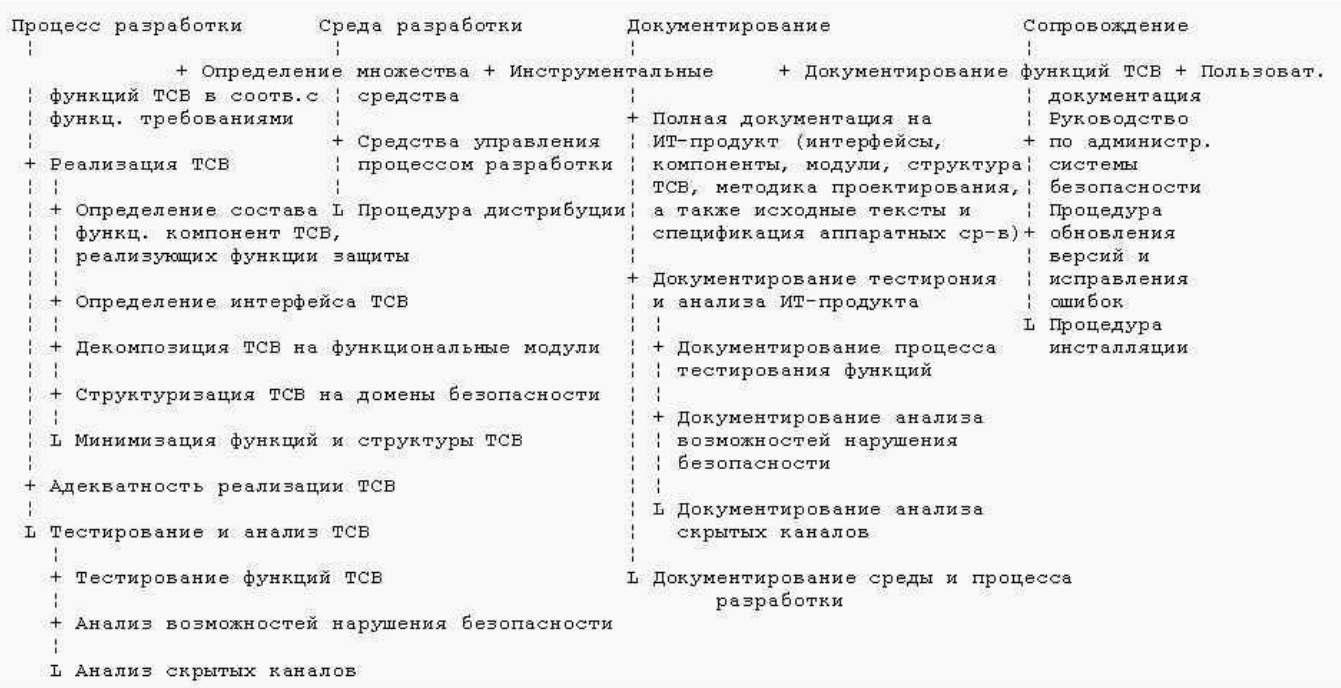

Рисунок 2 – Таксономия требований «Федеральных критериев» к технологии разработки ИТ-продукта

4 Требования к технологии разработки ИТ-продукта

Основное назначение требований к технологии разработки ИТ-продукта – обеспечить адекватность условий разработки функциональным требованиям, выдвинутым в соответствующем разделе профиля защиты, и установить ответственность разработчика за корректность реализации этих требований. Данный раздел регламентирует процесс создания, тестирования, документирования и сопровождения ИТ-продукта. Таксономия требований к технологии разработки ИТ-продукта приведена на рисунке 2.

«Федеральные критерии» содержат ранжированный перечень типовых требований к технологии разработки ИТ-продуктов. Выполнение требований к технологии разработки является необходимым условием для проведения процедуры квалификационного анализа.

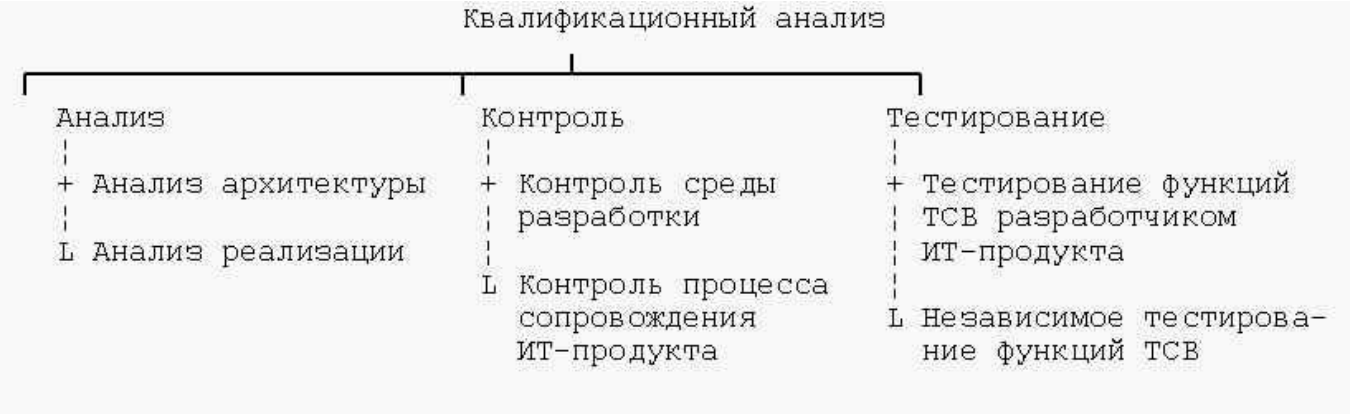

Рисунок 3 – Таксономия требований «Федеральных критериев» к процессу квалификационного анализа ИТ- продукта

5 Требования к процессу квалификационного анализа ИТ-продукта

Требования к процессу квалификационного анализа ИТ-продукта призваны обеспечить надежность и корректность этого процесса. Раздел содержит три группы требований, регламентирующих анализ, контроль и тестирование ИТ-продукта. Таксономия требований этого раздела приведена на рисунке 3.

Эти требования регламентируют процесс квалификационного анализа только в общих чертах и, по замыслу разработчиков стандарта, должны послужить основой для разработки специализированных методик квалификации уровня безопасности, ориентированных на различные области применения и типы ИТ-продуктов.

Тема 1.4 Канадские критерии безопасности компьютерных систем «CTCPEC»

1 Канадские критерии безопасности компьютерных систем «CTCPEC»

«Канадские критерии» разрабатывались для использования в качестве национального стандарта безопасности компьютерных систем. В отличие от «Оранжевой книги», ориентированной в основном на разработку и сертификацию многопользовательских операционных систем и требующей определенной интерпретации для других применений (например, для баз данных и сетей), «Канадские критерии» были изначально нацелены на широкий диапазон компьютерных систем. Этот стандарт может быть использован для разработки требований безопасности, спецификаций средств защиты и сертификации программного обеспечения рабочих станций и многопроцессорных вычислительных систем, персональных и многопользовательских операционных систем, систем управления базами данных, распределенных, сетевых, встроенных, объектно-ориентированных и других систем.

Возможность применения «Канадских критериев» к такому широкому кругу различных по назначению систем определяется используемым в них принципом дуального представления требований безопасности в виде функциональных требований к средствам защиты и требований к адекватности их реализации.

Функциональные критерии представляют собой частные метрики, предназначенные для определения показателей эффективности средств защиты в виде уровня их возможностей по отражению угроз соответствующего типа. Функциональные критерии разделяются на четыре группы: критерии конфиденциальности, целостности, работоспособности и аудита.

1) Критерии конфиденциальности включают:

- контроль скрытых каналов (три уровня);
- произвольное управление доступом (четыре уровня);
- нормативное управление доступом (четыре уровня);
- повторное использование объектов (один уровень).

2) Критерии целостности включают:
- домены целостности (два уровня);
- произвольное управление целостностью (четыре уровня);
- нормативное управление целостностью (четыре уровня);
- физическую целостность (четыре уровня);
- возможность осуществления отката (два уровня);
- разделение ролей (три уровня);
- самотестирование (три уровня).

3) Критерии работоспособности включают:
- контроль за распределением ресурсов (три уровня);
- устойчивость к отказам и сбоям (три уровня);
- живучесть (три уровня);
- восстановление (три уровня).

4) Критерии аудита включают:
- регистрацию и учет событий в системе (три уровня);
- идентификацию и аутентификацию (три уровня);
- прямое взаимодействие с ядром безопасности (три уровня). Ранжирование по уровням (выше приведено число уровней, не считая нулевого) внутри каждой группы критериев производится на основании мощности используемых методов защиты и класса отражаемых угроз соответствующего типа. Уровни с большим номером обеспечивают более полную функциональность и, соответственно, более высокую степень безопасности.

Адекватность реализации определяется тем, насколько точно и последовательно средства защиты реализуют принятую в компьютерной системе политику безопасности. Согласно «Канадским критериям», политика безопасности представляет собой множество правил, регламентирующих обработку, хранение и использование информации. Критерии адекватности рассматриваются без разделения на подгруппы и

определяют требования к процессу проектирования и разработки компьютерной системы. Уровень адекватности (от 0 до 7) присваивается всей системе в целом, причем более высокий уровень означает более полную и корректную реализацию политики безопасности.

Таким образом, «Канадские критерии» определяют степень безопасности компьютерной системы как совокупность функциональных возможностей используемых средств защиты, характеризующуюся частными показателями обеспечиваемого уровня безопасности, и одного обобщенного параметра – уровня адекватности реализации политики безопасности.

В состав приложений к «Канадским критериям» входят руководства по применению функциональных критериев и критериев адекватности реализации, а также подробное описание предложенной в них концепции обеспечения безопасности информации. Имеется приложение, включающее набор стандартных профилей защиты, содержащих типовые наборы требований к компьютерным системам, применяющимся в государственных учреждениях. Этот подход имеет много общего с концепцией профилей защиты, предлагаемой в «Федеральных критериях» США.

Тема 1.5 Гармонизированные критерии Европейских стран

1 Гармонизированные критерии Европейских стран

Изложение «Гармонизированных критериев» основывается на версии 1.2, опубликованной в июне 1991 года от имени соответствующих органов четырех стран – Франции, Германии, Нидерландов и Великобритании.

Принципиально важной чертой Европейских Критериев является отсутствие требований к условиям, в которых должна работать информационная система. Так называемый спонсор, то есть организация, запрашивающая сертификационные услуги, формулирует цель оценки, то есть описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции. Задача органа сертификации - оценить, насколько полно достигаются поставленные цели, то есть насколько корректны и эффективны архитектура и реализация механизмов безопасности в описанных спонсором условиях. Таким образом, в терминологии «Оранжевой книги», Европейские Критерии относятся к гарантированности безопасной работы системы. Требования к политике безопасности и наличию защитных механизмов не являются составной частью Критериев. Впрочем, чтобы облегчить формулировку цели оценки, Критерии содержат в качестве приложения описание десяти классов функциональности, типичных для правительственных и коммерческих систем.

Европейские Критерии рассматривают все основные составляющие информационной безопасности - конфиденциальность, целостность, доступность.

В Критериях проводится различие между системами и продуктами. Система – это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении. Продукт – это аппаратно-программный «пакет», который можно купить и по своему усмотрению встроить в ту или иную систему. Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь

угодно детально, а продукт должен быть рассчитан на использование в различных условиях.

Из практических соображений важно обеспечить единство критериев оценки продуктов и систем – например, чтобы облегчить оценку системы, составленной из ранее сертифицированных продуктов. По этой причине для систем и продуктов вводится единый термин – объект оценки.

Каждая система и (или) продукт предъявляет свои требования к обеспечению конфиденциальности, целостности и доступности. Чтобы удовлетворить эти требования, необходимо предоставить соответствующий набор функций (сервисов) безопасности, таких как идентификация и аутентификация, управление доступом или восстановление после сбоев.

Сервисы безопасности реализуются посредством конкретных механизмов. Чтобы объекту оценки можно было доверять, необходима определенная степень уверенности в наборе функций и механизмов безопасности. Степень уверенности мы будем называть гарантированностью. Гарантированность может быть большей или меньшей в зависимости от тщательности проведения оценки.

Гарантированность затрагивает два аспекта - эффективность и корректность средств безопасности. При проверке эффективности анализируется соответствие между целями, сформулированными для объекта оценки, и имеющимся набором функций безопасности. Точнее говоря, рассматриваются вопросы адекватности функциональности, взаимной согласованности функций, простоты их использования, а также возможные последствия эксплуатации известных слабых мест защиты. Кроме того, в понятие эффективности входит способность механизмов защиты противостоять прямым атакам (мощность механизма). Определяются три градации мощности – базовая, средняя и высокая.

Под корректностью понимается правильность реализации функций и механизмов безопасности. В Критериях определяется семь возможных уровней гарантированности корректности – от E0 до E6 (в порядке возрастания). Уровень E0 означает отсутствие гарантированности. При проверке корректности анализируется

весь жизненный цикл объекта оценки – от проектирования до эксплуатации и сопровождения.

Общая оценка системы складывается из минимальной мощности механизмов безопасности и уровня гарантированности корректности.

Гармонизированные критерии Европейских стран явились для своего времени весьма передовым стандартом, они создали предпосылки для появления «Общих критериев».

Тема 1.6 Интерпретация «Оранжевой книги» (TCSEC) для сетевых конфигураций

1 Интерпретация «Оранжевой книги» (TCSEC) для сетевых конфигураций

В 1987 году Национальный центр компьютерной безопасности США выпустил в свет интерпретацию «Оранжевой книги» для сетевых конфигураций. Документ состоит из двух частей.

Первая содержит собственно интерпретацию, во второй рассматриваются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

Основные положения интерпретации «Оранжевой книги» сводятся к следующему.

В первой части вводится минимум новых понятий. Важнейшее из них – безопасная сетевая компьютерная система.

Нет прямой зависимости между уровнями безопасности отдельных компонентов и уровнями безопасности всей сетевой конфигурации.

Управление доступом осуществляется с учетом сетевых структур.

Идентификация групп пользователей может строиться на основе сетевых адресов хостов или (под)сетей.

Возможен централизованный контроль доступа, когда решение принимает специальный сервер авторизации. Аналогично идентификация и аутентификация пользователей может производиться как централизованно (соответствующим сервером), так и локально – той системой, с которой пользователь непосредственно взаимодействует.

Расширяется регистрационная информация. Возможно выделение в сети одного или нескольких серверов протоколирования и аутентификации.

Учет динамичности сетевых конфигураций, в том числе, в «Руководстве администратора по средствам безопасности».

Повышенное внимание к целостности информации вообще и меток безопасности в частности.

Если первая часть Интерпретации посвящена в основном управлению доступом к информации, то во второй нашли отражение все основные аспекты безопасности – конфиденциальность, целостность и доступность.

В Интерпретации приведены новые сервисы безопасности и защитные механизмы.

Среди защитных механизмов в сетевых конфигурациях на первом месте стоит криптография, помогающая поддерживать как конфиденциальность, так и целостность. Следствием является необходимость реализации механизмов управления ключами.

Для поддержания целостности (в аспектах, относящихся к коммуникациям) используются аутентификация, контроль целостности полей и механизмы обеспечения неотказуемости.

Новым является рассмотрение вопросов доступности. Сетевой сервер перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или функциональный сервер не в состоянии обслужить запросы.

Критерии части 2 дополняют «Оранжевую книгу». Каждый сервис безопасности рассматривается независимо и может получить одну из трех положительных оценок. Таким образом, общая оценка сетевой конфигурации выглядит примерно так: класс безопасности С2, сервис_1 – удовлетворительно; сервис_2 – «хорошо» и пр. Заказчик, зная свои потребности, в состоянии принять решение о пригодности той или иной конфигурации.

2 Сетевая доверенная вычислительная база

Важнейшее понятием, приводимым ы первой части является (в том числе) – сетевая доверенная вычислительная база, распределенный аналог доверенной вычислительной базы изолированных систем. Сетевая доверенная вычислительная база формируется из всех частей всех компонентов сети, обеспечивающих информационную безопасность. Доверенная сетевая система должна обеспечивать такое распределение защитных механизмов, чтобы общая политика безопасности реализовывалась, несмотря на уязвимость коммуникационных путей и на параллельную, асинхронную работу компонентов.

Прямой зависимости между вычислительными базами компонентов, рассматриваемых как изолированные системы, и фрагментами сетевой вычислительной базы не существует. Более того, нет прямой зависимости и между уровнями безопасности отдельных компонентов и уровнем безопасности всей сетевой конфигурации. Например, в результате объединения двух систем класса B1, обладающих несовместимыми правилами кодирования меток безопасности, получается сеть, не удовлетворяющая требованию целостности меток. В качестве противоположного примера рассмотрим объединение двух компонентов, один из которых сам не обеспечивает протоколирование действий пользователя, но передает необходимую информацию другому компоненту, который и ведет протокол. В таком случае распределенная система в целом, несмотря на слабость компонента, удовлетворяет требованию подотчетности.

Чтобы понять суть положений, вошедших в первую часть, рассмотрим интерпретацию требований к классу безопасности C2. Первое требование к этому классу – поддержка произвольного управления доступом. Интерпретация предусматривает различные варианты распределения сетевой доверенной вычислительной базы по компонентам и, соответственно, различные варианты распределения механизмов управления доступом. В частности, некоторые компоненты, закрытые для прямого доступа пользователей, могут вообще не содержать подобных механизмов.

Интерпретация отличается от самих «Критериев» учетом динамичности сетевых конфигураций. Предусматривается наличие средств проверки подлинности и корректности функционирования компонентов перед их включением в сеть, наличие протокола взаимной проверки компонентами корректности функционирования друг друга, а также присутствие средств оповещения администратора о неполадках в сети. Сетевая конфигурация должна быть устойчива к отказам отдельных компонентов или коммуникационных путей.

Среди защитных механизмов в сетевых конфигурациях на первом месте стоит криптография, помогающая поддерживать как конфиденциальность, так и целостность. Следствием использования криптографических методов является необходимость реализации механизмов управления ключами.

Систематическое рассмотрение вопросов доступности является новшеством по сравнению не только с «Оранжевой книгой», но и с рекомендациями X.800. Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в обслуживании пользователей. Доверенная система должна иметь возможность обнаруживать ситуации недоступности, уметь возвращаться к нормальной работе и противостоять атакам на доступность.

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

– внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т.п.);

– наличие средств реконфигурирования для изоляции и/или замены узлов или коммуникационных каналов, отказавших или подвергшихся атаке на доступность;

– рассредоточенность сетевого управления, отсутствие единой точки отказа;

– наличие средств нейтрализации отказов (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов);

– выделение подсетей и изоляция групп пользователей друг от друга.

Одним из важнейших в «Оранжевой книге» является понятие монитора обращений. Применительно к структурированию сетевой конфигурации можно сформулировать следующее утверждение, обеспечивающее достаточное условие корректности фрагментирования монитора обращений.

Пусть каждый субъект (то есть процесс, действующий от имени какого-либо пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Далее, пусть каждый компонент содержит свой монитор обращений, отслеживающий все локальные попытки доступа, и все мониторы реализуют согласованную политику безопасности. Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый монитор обращений для всей сетевой конфигурации.

Данное утверждение является теоретической основой декомпозиции распределенной ИС в объектно-ориентированном стиле в сочетании с криптографической защитой коммуникаций.