Обзор международных и национальных стандартов и спецификаций в области ИБ: «Оранжевая книга», ИСО 15408

Основные сведения

**Критерии оценки доверенных компьютерных систем** — стандарт [Министерства обороны](https://ru.wikipedia.org/wiki/%D0%9C%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D0%B5%D1%80%D1%81%D1%82%D0%B2%D0%BE_%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D1%8B_%D0%A1%D0%A8%D0%90) [США](https://ru.wikipedia.org/wiki/%D0%A1%D0%A8%D0%90) ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *Department of Defense Trusted Computer System Evaluation Criteria, TCSEC*, DoD 5200.28-STD, December 26, 1985), более известный под именем «Оранжевая книга» ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *"Orange Book"*) из-за цвета обложки.

Данный стандарт получил международное признание и оказал исключительно сильное влияние на последующие разработки в области [информационной безопасности](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C) (ИБ).

Данный стандарт относится к оценочным стандартам (классификация [информационных систем](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) и [средств защиты](https://ru.wikipedia.org/w/index.php?title=%D0%A1%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B2%D0%BE_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B&action=edit&redlink=1)) и речь в нём идёт не о безопасных, а о [доверенных системах](https://ru.wikipedia.org/w/index.php?title=%D0%94%D0%BE%D0%B2%D0%B5%D1%80%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0&action=edit&redlink=1).

Каких-либо абсолютных систем (в том числе и безопасных) в нашей жизни не существует. Поэтому и было предложено оценивать лишь степень доверия, которое можно оказать той или иной системе.

В стандарте заложен понятийный базис ИБ ([безопасная система](https://ru.wikipedia.org/w/index.php?title=%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0&action=edit&redlink=1), [доверенная система](https://ru.wikipedia.org/w/index.php?title=%D0%94%D0%BE%D0%B2%D0%B5%D1%80%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0&action=edit&redlink=1), [политика безопасности](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8), [уровень гарантированности](https://ru.wikipedia.org/w/index.php?title=%D0%A3%D1%80%D0%BE%D0%B2%D0%B5%D0%BD%D1%8C_%D0%B3%D0%B0%D1%80%D0%B0%D0%BD%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D0%B8&action=edit&redlink=1), [подотчетность](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D0%BE%D0%B4%D0%BE%D1%82%D1%87%D0%B5%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C&action=edit&redlink=1), [доверенная вычислительная база](https://ru.wikipedia.org/w/index.php?title=%D0%94%D0%BE%D0%B2%D0%B5%D1%80%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B0%D0%B7%D0%B0&action=edit&redlink=1), [монитор обращений](https://ru.wikipedia.org/w/index.php?title=%D0%9C%D0%BE%D0%BD%D0%B8%D1%82%D0%BE%D1%80_%D0%BE%D0%B1%D1%80%D0%B0%D1%89%D0%B5%D0%BD%D0%B8%D0%B9&action=edit&redlink=1), [ядро безопасности](https://ru.wikipedia.org/w/index.php?title=%D0%AF%D0%B4%D1%80%D0%BE_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8&action=edit&redlink=1), [периметр безопасности](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D0%B5%D1%80%D0%B8%D0%BC%D0%B5%D1%82%D1%80_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8&action=edit&redlink=1)).

Безопасность и доверие оцениваются в данном стандарте с точки зрения управления доступом к информации, что и является средством обеспечения [конфиденциальности](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C) и [целостности](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8).

Вслед за «Оранжевой книгой» появилась целая «[Радужная серия](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D1%83%D0%B6%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%80%D0%B8%D1%8F)». Наиболее значимой в ней явилась интерпретация «Оранжевой книги» для сетевых конфигураций ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *National Computer Security Center. Trusted Network Interpretation*, NCSC-TG-005, 1987), где в первой части интерпретируется «Оранжевая книга», а во второй части описываются сервисы безопасности, специфичные для сетевых конфигураций.

Основные цели и средства

**Политики**

Политики безопасности должны быть подробными, чётко определёнными и обязательными для компьютерной системы. Есть две основных политики безопасности:

* Мандатная политика безопасности — обязательные правила управления доступом напрямую, основанные на индивидуальном разрешении, разрешении на доступ к информации и уровне конфиденциальности запрашиваемой информации. Другие косвенные факторы являются существенными и окружающими. Эта политика также должна точно соответствовать закону, главной политике и прочим важным руководствам, в которых устанавливаются правила.
  + Маркирование — системы, предназначенные для обязательной мандатной политики безопасности, должны предоставлять и сохранять целостность меток управления доступом, а также хранить метки, если объект перемещён.
* Дискреционная политика безопасности — предоставляет непротиворечивый набор правил для управления и ограничения доступа, основанный на идентификации тех пользователей, которые намерены получить только необходимую им информацию.

**Ответственность**

Индивидуальная ответственность в независимости от политики должна быть обязательной. Есть три требования по условиям ответственности:

* [Аутентификация](https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) — процесс, используемый для распознавания индивидуального пользователя.
* [Авторизация](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) — проверка разрешения индивидуальному пользователю на получение информации определённого рода.
* Аудит — контролируемая информация должна избирательно храниться и защищаться в мере, достаточной для отслеживания действий аутентифицированного пользователя, затрагивающих безопасность.

**Гарантии**

Компьютерная система должна содержать аппаратные и/или программные механизмы, которые могут независимо определять, обеспечивается ли достаточная уверенность в том, что система исполняет указанные выше требования. Вдобавок уверенность должна включать гарантию того, что безопасная часть системы работает только так, как запланировано. Для достижения этих целей необходимо два типа гарантий и соответствующих им элементов:

**Механизмы гарантий**

***Операционная гарантия*** — уверенность в том, что реализация спроектированной системы обеспечивает осуществление принятой стратегии защиты системы. Сюда относятся системная архитектура, целостность системы, анализ скрытых каналов, безопасное управление возможностями и безопасное восстановление.

***Гарантия жизненного цикла*** — уверенность в том, что система разработана и поддерживается в соответствии с формализованными и жёстко контролируемыми критериями функционирования. Сюда относятся тестирование безопасности, задание на проектирование и его проверка, управление настройками и соответствие параметров системы заявленным.

***Гарантии непрерывной защиты*** — надёжные механизмы, обеспечивающие непрерывную защиту основных средств от преступных и/или несанкционированных изменений.

**Документирование**

В каждом классе есть дополнительный набор документов, который адресован разработчикам, пользователям и администраторам системы в соответствии с их полномочиями. Эта документация содержит:

* Руководство пользователя по особенностям безопасности.
* Руководство по безопасным средствам работы.
* Документация о тестировании.
* Проектная документация

Основные понятия

**Безопасная система**

Это система, которая обеспечивает управление доступом к информации таким образом, что только авторизованные лица или процессы, действующие от их имени, получают право работы с информацией.

**Доверенная система**

Под доверенной системой в стандарте понимается система, использующая аппаратные и программные средства для обеспечения одновременной обработки информации разной категории секретности группой пользователей без нарушения прав доступа.

**Политика безопасности**

Это набор законов, правил, процедур и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. Причём, политика безопасности относится к активным методам защиты, поскольку учитывает анализ возможных угроз и выбор адекватных мер противодействия.

**Уровень гарантированности**

Подразумевает меру доверия, которая может быть оказана архитектуре и реализации информационной системы, и показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности (пассивный аспект защиты).

**Подотчетность**

В группе «Подотчетность» должны быть следующие требования:

* **1) Идентификация и аутентификация.** Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентификации) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и должны быть ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.
* **2) Регистрация и учет.** Для определения степени ответственности пользователей за действия в системе, все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищённом протоколе (то есть должен существовать объект компьютерной системы, потоки от которого и к которому доступны только субъекту администрирования). Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объёма протокола и повышения эффективности его анализа. Протокол событий должен быть надёжно защищён от несанкционированного доступа, модификации и уничтожения.

**Доверенная вычислительная база**

Это совокупность защитных механизмов информационной системы (как программные, так и аппаратные), реализующих политику безопасности.

**Монитор обращений**

Контроль за выполнением субъектами (пользователями) определённых операций над объектами, путём проверки допустимости обращения (данного пользователя) к программам и данным разрешенному набору действий.

Обязательные качества для монитора обращений:

1. Изолированность (неотслеживаемость работы).
2. Полнота (невозможность обойти).
3. Верифицируемость (возможность анализа и тестирования).

**Ядро безопасности**

Конкретная реализация монитора обращений, обладающая гарантированной неизменностью.

**Периметр безопасности**

Это граница доверенной вычислительной базы.

Механизмы реализации безопасности

**Произвольное управление доступом**

Иначе — добровольное управление доступом.

*Добровольное управление доступом* — это метод ограничения доступа к объектам, основанный на учёте личности субъекта или группы, в которую субъект входит. Добровольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению давать другим субъектам или отбирать у них права доступа к объекту.

Большинство операционных систем и СУБД реализуют именно добровольное управление доступом. Главное его достоинство — гибкость, главные недостатки — рассредоточенность управления и сложность централизованного контроля, а также оторванность прав доступа от данных, что позволяет копировать секретную информацию в общедоступные файлы или секретные файлы в незащищённые каталоги.

**Безопасность повторного использования объектов**

Безопасность повторного использования объектов — важное на практике дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения секретной 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. Важно обратить внимание на следующий момент. Поскольку информация о субъектах также представляет собой объект, необходимо позаботиться о безопасности «повторного использования субъектов». Когда пользователь покидает организацию, следует не только лишить его возможности входа в систему, но и запретить доступ ко всем объектам. В противном случае, новый сотрудник может получить ранее использовавшийся идентификатор, а с ним и все права своего предшественника.

Современные интеллектуальные периферийные устройства усложняют обеспечение безопасности повторного использования объектов. Действительно, принтер может буферизовать несколько страниц документа, которые останутся в памяти даже после окончания печати. Необходимо предпринять специальные меры, чтобы «вытолкнуть» их оттуда.

**Метки безопасности**

Предусмотрены метки для субъектов (степень благонадёжности) и объектов (степень конфиденциальности информации). Метки безопасности содержат данные об уровне секретности и категории, к которой относятся данные. Согласно «Оранжевой книге», метки безопасности состоят из двух частей — уровня секретности и списка категорий. Уровни секретности, поддерживаемые системой, образуют упорядоченное множество, которое может выглядеть, например, так:

* совершенно секретно;
* секретно;
* конфиденциально;
* не секретно.

Для разных систем набор уровней секретности может различаться. Категории образуют неупорядоченный набор. Их назначение — описать предметную область, к которой относятся данные. В военном окружении каждая категория может соответствовать, например, определённому виду вооружений. Механизм категорий позволяет разделить информацию по отсекам, что способствует лучшей защищённости. Субъект не может получить доступ к «чужим» категориям, даже если его уровень благонадёжности «совершенно секретно». Специалист по танкам не узнает тактико-технические данные самолётов.

Главная проблема, которую необходимо решать в связи с метками, это обеспечение их целостности. Во-первых, не должно быть непомеченных субъектов и объектов, иначе в меточной безопасности появятся легко используемые бреши. Во-вторых, при любых операциях с данными метки должны оставаться правильными. В особенности это относится к экспорту и импорту данных. Например, печатный документ должен открываться заголовком, содержащим текстовое и/или графическое представление метки безопасности. Аналогично при передаче файла по каналу связи должна передаваться и ассоциированная с ним метка, причём в таком виде, чтобы удалённая система могла её разобрать, несмотря на возможные различия в уровнях секретности и наборе категорий.

Одним из средств обеспечения целостности меток безопасности является разделение устройств на многоуровневые и одноуровневые. На многоуровневых устройствах может храниться информация разного уровня секретности (точнее, лежащая в определённом диапазоне уровней). Одноуровневое устройство можно рассматривать как вырожденный случай многоуровневого, когда допустимый диапазон состоит из одного уровня. Зная уровень устройства, система может решить, допустимо ли записывать на него информацию с определённой меткой. Например, попытка напечатать совершенно секретную информацию на принтере общего пользования с уровнем «несекретно» потерпит неудачу.

**Принудительное управление доступом**

Принудительное 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. Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, «конфиденциальный» субъект может писать в секретные файлы, но не может — в несекретные (разумеется, должны также выполняться ограничения на набор категорий). На первый взгляд подобное ограничение может показаться странным, однако оно вполне разумно. Ни при каких операциях уровень секретности информации не должен понижаться, хотя обратный процесс вполне возможен.

Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов, на месте которых могут оказаться даже системные администраторы. После того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа. В терминах принудительного управления нельзя выразить предложение «разрешить доступ к объекту Х ещё и для пользователя Y». Конечно, можно изменить метку безопасности пользователя Y, но тогда он скорее всего получит доступ ко многим дополнительным объектам, а не только к Х.

Принудительное управление доступом реализовано во многих вариантах операционных систем и СУБД, отличающихся повышенными мерами безопасности. В частности, такие варианты существуют для SunOS и СУБД Ingres. Независимо от практического использования принципы принудительного управления являются удобным методологическим базисом для начальной классификации информации и распределения прав доступа. Удобнее мыслить в терминах уровней секретности и категорий, чем заполнять неструктурированную матрицу доступа. Впрочем, в реальной жизни добровольное и принудительное управление доступом сочетается в рамках одной системы, что позволяет использовать сильные стороны обоих подходов.

Разделы и классы

Критерии делятся на 4 раздела: D, C, B и A, из которых наивысшей безопасностью обладает раздел A. Каждый дивизион представляет собой значительные отличия в доверии индивидуальным пользователям или организациям. Разделы C, B и A иерархически разбиты на серии подразделов, называющиеся классами: C1, C2, B1, B2, B3 и A1. Каждый раздел и класс расширяет или дополняет требования указанные в предшествующем разделе или классе.

**D — Минимальная защита**

Системы, безопасность которых была оценена, но оказалась не удовлетворяющей требованиям более высоких разделов.

**C — Дискреционная защита**C1 — Дискреционное обеспечение секретности.

* + Разделение пользователей и данных
  + [Дискреционное управление доступом](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D0%BA%D1%80%D0%B5%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B5_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC), допускающее принудительное ограничение доступа на индивидуальной основе.
* C2 — Управление доступом
  + Более чётко оформленное дискреционное управление доступом.
  + Индивидуальные учётные записи, вход под которыми возможен через процедуру авторизации.
  + Журнал контроля доступа к системе.
  + Изоляция ресурсов.

**B — Мандатная защита**

* B1 — Защита с применением мета-безопасности
  + [Мандатное управление доступом](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D0%BD%D0%B4%D0%B0%D1%82%D0%BD%D0%BE%D0%B5_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC) к выбранным субъектам и объектам.
  + Все обнаруженные недостатки должны быть устранены или убраны каким-либо другим способом.
  + Маркировка данных
* B2 — Структурированная защита
  + Чётко определённая и документированная модель правил безопасности.
  + Применение расширенного дискреционного и мандатного управления доступом ко всем объектам и субъектам.
  + Скрытые каналы хранения.
* B3 — Домены безопасности
  + Соответствие требованиям [монитора обращений](https://ru.wikipedia.org/w/index.php?title=%D0%9C%D0%BE%D0%BD%D0%B8%D1%82%D0%BE%D1%80_%D0%BE%D0%B1%D1%80%D0%B0%D1%89%D0%B5%D0%BD%D0%B8%D0%B9&action=edit&redlink=1).
  + Структурирование для исключения кода, не отвечающего требованиям обязательной политики безопасности.
  + Поддержка администратора системы безопасности.
  + Примером подобной системы является [XTS-300](https://ru.wikipedia.org/w/index.php?title=XTS-300&action=edit&redlink=1), предшественница [XTS-400](https://ru.wikipedia.org/wiki/XTS-400).

**A — Проверенная защита**

* A1 — Проверенный дизайн.
  + По функциям идентично B3.
  + Формализованный дизайн и проверенные техники, включающие высокоуровневую спецификацию.
  + Формализованные процедуры управления и распространения.
  + Примером подобной системы является [SCOMP](https://ru.wikipedia.org/w/index.php?title=SCOMP&action=edit&redlink=1), предшественница XTS-400.
* Выше A1
  + Системная архитектура демонстрирующая, что требования самозащиты и полноценности для мониторов обращений были выполнены в соответствии с «Базой безопасных вычислений» (коллекцией программного и аппаратного обеспечения необходимых для обязательной политики безопасности в операционных системах ориентированных на безопасность).

Классы безопасности

В критериях впервые введены четыре уровня доверия — D, C, B и A, которые подразделяются на классы. Классов безопасности всего шесть — C1, C2, B1, B2, B3, A1 (перечислены в порядке ужесточения требований).

**Уровень D**

Данный уровень предназначен для систем, признанных неудовлетворительными.

**Уровень C**

Иначе — произвольное управление доступом.

**Класс C1**

Политика безопасности и уровень гарантированности для данного класса должны удовлетворять следующим важнейшим требованиям:

1. доверенная вычислительная база должна управлять доступом именованных пользователей к именованным объектам;
2. пользователи должны идентифицировать себя, причём аутентификационная информация должна быть защищена от несанкционированного доступа;
3. доверенная вычислительная база должна поддерживать область для собственного выполнения, защищённую от внешних воздействий;
4. должны быть в наличии аппаратные или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов доверенной вычислительной базы;
5. защитные механизмы должны быть протестированы (нет способов обойти или разрушить средства защиты доверенной вычислительной базы);
6. должны быть описаны подход к безопасности и его применение при реализации доверенной вычислительной базы.

**Класс C2**

В дополнение к C1:

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

**Уровень B**

Также именуется — принудительное управление доступом.

**Класс B1**

В дополнение к C2:

1. доверенная вычислительная база должна управлять метками безопасности, ассоциируемыми с каждым субъектом и хранимым объектом.
2. доверенная вычислительная база должна обеспечить реализацию принудительного управления доступом всех субъектов ко всем хранимым объектам.
3. доверенная вычислительная база должна обеспечивать взаимную изоляцию процессов путём разделения их адресных пространств.
4. группа специалистов, полностью понимающих реализацию доверенной вычислительной базы, должна подвергнуть описание архитектуры, исходные и объектные коды тщательному анализу и тестированию.
5. должна существовать неформальная или формальная модель политики безопасности, поддерживаемой доверенной вычислительной базой.

**Класс B2**

В дополнение к B1:

1. снабжаться метками должны все ресурсы системы (например, ПЗУ), прямо или косвенно доступные субъектам.
2. к доверенной вычислительной базе должен поддерживаться доверенный коммуникационный путь для пользователя, выполняющего операции начальной идентификации и аутентификации.
3. должна быть предусмотрена возможность регистрации событий, связанных с организацией тайных каналов обмена с памятью.
4. доверенная вычислительная база должна быть внутренне структурирована на хорошо определённые, относительно независимые модули.
5. системный архитектор должен тщательно проанализировать возможности организации тайных каналов обмена с памятью и оценить максимальную пропускную способность каждого выявленного канала.
6. должна быть продемонстрирована относительная устойчивость доверенной вычислительной базы к попыткам проникновения.
7. модель политики безопасности должна быть формальной. Для доверенной вычислительной базы должны существовать описательные спецификации верхнего уровня, точно и полно определяющие её интерфейс.
8. 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.
9. тесты должны подтверждать действенность мер по уменьшению пропускной способности тайных каналов передачи информации.

**Класс B3**

В дополнение к B2:

1. для произвольного управления доступом должны обязательно использоваться списки управления доступом с указанием разрешённых режимов.
2. 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.
3. доверенная вычислительная база должна быть спроектирована и структурирована таким образом, чтобы использовать полный и концептуально простой защитный механизм с точно определённой семантикой.
4. процедура анализа должна быть выполнена для временных тайных каналов.
5. должна быть специфицирована роль администратора безопасности. Получить права администратора безопасности можно только после выполнения явных, протоколируемых действий.
6. должны существовать процедуры и/или механизмы, позволяющие произвести восстановление после сбоя или иного нарушения работы без ослабления защиты.
7. должна быть продемонстрирована устойчивость доверенной вычислительной базы к попыткам проникновения.

**Уровень A**

Носит название — верифицируемая безопасность.

**Класс A1**

В дополнение к B3:

1. тестирование должно продемонстрировать, что реализация доверенной вычислительной базы соответствует формальным спецификациям верхнего уровня.
2. помимо описательных, должны быть представлены формальные спецификации верхнего уровня. Необходимо использовать современные методы формальной спецификации и верификации систем.
3. механизм конфигурационного управления должен распространяться на весь [жизненный цикл](https://ru.wikipedia.org/wiki/%D0%96%D0%B8%D0%B7%D0%BD%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D1%86%D0%B8%D0%BA%D0%BB_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B) и все компоненты системы, имеющие отношение к обеспечению безопасности.
4. должно быть описано соответствие между формальными спецификациями верхнего уровня и исходными текстами.

Краткая классификация

Такова классификация, введённая в «Оранжевой книге». Коротко её можно сформулировать так:

* уровень C — произвольное управление доступом;
* уровень B — принудительное управление доступом;

Конечно, в адрес «Критериев …» можно высказать целый ряд серьёзных замечаний (таких, например, как полное игнорирование проблем, возникающих в распределённых 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 остаётся 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.

* [Army Regulation 380-19 — пример руководства по определению того, система какого класса должна использоваться в конкретной ситуации.](http://www.fas.org/irp/doddir/army/r380_19.pdf)
* *Домарев В. В., к. т. н.* [Оценка эффективности систем защиты информации.](http://citforum.ru/security/articles/model_proc/)