Санкт-Петербургский Государственный Университет,
Физический Факультет.

Курсовая работа
по информатике.

Воропаев Роман Алексеевич,
105 группа направления ПМФ.

Санкт-Петербург, 2008.

Стандарты информационной безопасности

согласно

US Department of Defense

Trusted Computer System Evaluation Criteria.

Вступление.

Вопросы информационной безопасности играют сегодня огромную роль в сфере высоких технологий, где именно информация (особенно цифровая) становится одновременно «продуктом и сырьём». Огромный мегаполис IT построен на всемирных реках данных из разных точек планеты. Её производят, обрабатывают, продают и, к сожалению, зачастую воруют.

Потому жизненно необходимы методы защиты информации для любого человека современной цивилизации, особенно использующего компьютер. По этой причине практически любой пользователь ПК в мире так или иначе «подкован» в вопросах борьбы с вирусами, «троянскими конями» и другими вредоносными програмами, а также личностями стоящими за их созданием и распространением — взломщиками, спамерами, крэкерами, вирусмэйкерами (создателями вирусов) и просто мошенниками , обманывающих людей в поисках наживы — корпоративной информации, стоящей немалых денег.

Причём последние зачастую осуществляют задуманное руками своих жертв. А потому «технические» и «физические» методы защиты информации должны совмещаться с образованием пользователей в области компьютерных технологий и в часности компьютерной безопасности.

Одними из первых эти проблемы осознали и предприняли решительный шаг к их решению государственные ведомства США в конце 60-х годов, когда компьютеры стоили сотни тысяч долларов, а интернет зарождался из немногочисленых чисто военных и научных сетей.

История.

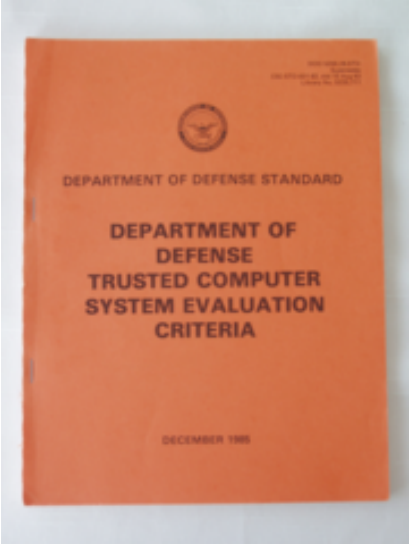
При объединении и синхронизации вышеупомянутых сетей остро встал вопрос защиты «от шпионов» секретной государственной информации, особенно учитывая то насколько
легко и быстро можно скопировать информацию в цифровом виде.

В 1967 под патронажем Национального Комитета Стандартов была учреждена Инициативная Группа исследователей по вопросам компьютерной безопасности, в которую вошли представители университетов, компаний по производству компьютеров, научно-исследовательских центров и других организаций.

Результатом объединения усилий промышленных и научных специалистов, множества теоретических исследований в широкой области математики — теории информации, а также огромного опыта в реальной индустрии, оказалась «радужная серия» - ряд стандартов и требований предъявляемых к оборудованию, програмному обеспечению и персоналу так называемых систем автоматической обработки данных — компьютерных сетей,принадлежавших таким гос. структурам США как : NASA, Министерство Обороны, Национальный комитет стандартов, Министерство Труда, Отдел по охране окружающей среды, Министерство по контролю за вооружением, Национальное научное общество, Федеральная резервная система и наконец Центр Объединенного Командования ВС.

Был даже создан Национальный Центр Компьютерной Безопасности, всецело занимавшийся этими вопросами.

А в 1981 был создан подобный центр при Министерстве Обороны, разработавший и внедривший «радужную серию» в 1985 году. Наиболее значимым для истории в силу своей общности и направленности не только на сугубо внутренние цели, но и на некую оценку качества коммерческих продуктов так или иначе обрабатывающих и хранящих конфеденциально важную информацию, стал стандарт «Критерии оценки доверенных компьютерных систем», названный Оранжевой книгой в силу цвета обложки (кстати говоря, оранжевую обложку имеет не только этот мировой стандарт — по меньшей мере спецификации на лазерный аудио-диск и на шейдерную модель OpenGL называют оранжевыми книгами). Её целью были максимальная гибкость и универсальность **оценки** безопасности.



Компьютерная безопасность.

Пожалуй, стоит начать с того, что же такое компьютерная безопасность. Наиболее общее определение можно сформулировать так:

Компьютерная безопасность — состояние полного контроля законных владельцев и пользователей вычислительной системы за входящими и выходящими потоками данных всей системы в целом и любого её элемента при полном и однозначном соответствии законам, мерам, политикам организаций, а главное -- поставленным задачам перед системой.

Ключевые слова в этом определении — полный контроль, означающие что в любой момент времени администратор (ч-к отвечающий за корректную работу системы в целом) или же офицер безопасности (security officer) знает или легко может установить явления и события, происходящие или произошедшие в системе, и при необходимости пресечь их с наименьшими потерями функциональности.

В этом аспекте компьютерная безопасность сходна с физической — например собаке, охраняющей дом хозяев. Она пускает или отпугивает входящих людей, руководствуясь правилами «свой — не свой», и в каждый момент знает кто вошел в дом, а кто вышел из него. Таким образом она, выражаясь языком ИБ, осуществляет контроль доступа к дому.

В самой Книге подобная концепция называется Монитором Отношений (Reference Monitor), подобно реальной охранной системе

отслеживающей все действия пользователей (т.е. процессов, действующих от их имени) связанные с внешним потенциально опасным миром.

Но в реальном мире, а не абстракном мире математики, этого не достаточно, поскольку сама операционная система (или база данных или ещё что-то) всегда содержит ошибки и недочёты, на нахождение которых ушло бы слишком много и без того драгоценного времени тестирования. И всегда существует вероятность, что ими могут воспользоваться намеренно или случайно, чтобы заставить систему «добровольно» выдать конфиденциальную информацию. Именно потому понятие Монитора Отношений конкретизируется, расширяется и дополняется Критериями, построенными по принципу иерархической классификации с постепенным ужесточением требований.

Также нельзя забывать, что компьютерная безопасность — процесс, а не готовый продукт. Т.е. нельзя предсказать и учесть все возможные угрозы, поэтому важна готовность персонала любого уровня разпознать и попытаться отразить доселе не ведомые виды вторжений.

Оказывается, что все эти идеи были заложены в Оранжевой книге еще 20 лет назад!

Структура Книги.

Сначала вводятся основные понятия, заложившие основу словаря информационной безопасности на десятилетия вперед.

Безопасная система(Secure system) - 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(Trusted system) - 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(Security policy) - это набор законов, правил, процедур и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. Причем, политика безопасности относится к активным методам защиты, поскольку учитывает анализ возможных угроз и выбор адекватных мер противодействия.

Уровень гарантированности (Assurance)- 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(Audit) - Доверенная система должна фиксировать все события (вести протокол), связанные с обеспечением безопасности информационной системы.

Доверенная вычислительная база(Trusted Computer Base) -

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

Монитор обращений(Reference Monitor) - **к**онтроль за выполнением субъектами (пользователями) определенных операций над объектами, путем 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(Security kernel) - конкретная реализация монитора обращений, обладающая гарантированной неизменностью.

Периметр безопасности(Security Perimeter) -это граница доверенной вычислительной базы.

Канал утечек/тайный канал - паразитический канал связи, возникающий в любом канале связи, позволяющий обойти контроль доступа к информации. Гл. метод борьбы — уменьшение их пропускной способности(bandwidth).

Механизмы защиты.

Для реализации вышеописанных понятий безопасной и доверенной системы используются следующие механизмы, реализуемые аппаратно или программно в доверенном вычислительном ядре.

Произвольное управление доступом

(Discretionary Access Control).

Иначе - добровольное управление доступом. *Добровольное управление доступом* - это метод ограничения доступа к объектам, основанный на учете 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 незащищенные каталоги.

Безопасность повторного использования объектов (Object Reuse).

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. Впрочем, иногда организации защищаются от повторного использования слишком ревностно - путем уничтожения магнитных носителей. На практике заведомо достаточно троекратной записи случайных последовательностей бит.

Метки безопасности(Security Labels).

Предусмотрены метки для субъектов (степень благонадежности) и объектов (степень конфиденциальности информации). Метки безопасности содержат данные об уровене 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; • несекретно.

Впрочем, 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, определенному виду вооружений. Механизм категорий позволяет разделить информацию по отсекам, что способствует лучшей защищенности. Субъект не может получить доступ к «чужим» категориям, даже если его уровень благонадежности «совершенно секретно». Специалист по танкам не узнает тактико-технические данные самолетов. 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, причем в таком виде, чтобы удаленная система могла ее 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 определенном диапазоне уровней). Зная уровень устройства, система может решить, допустимо ли записывать на него информацию с определенной меткой. Например, попытка напечатать совершенно секретную информацию на принтере общего пользования с уровнем «несекретно» потерпит неудачу.

Принудительное управление доступом

(Mandatory Access Control).

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" субьект 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 X еще 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 X. 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.

Классы безопасности.

Сама оценка безопасности основывается, как уже упоминалось, на иерарархической классификации. В оригинальном тексте каждый класс каждого уровня описывается с нуля, т.е. наследуемые требования с более низких классов каждый раз повторяются. Для сокращения далее приведены лишь различия, появляющиеся по возрастанию уровня «доверяемости». Всего 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 - «заваливших экзамен».

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, причем аутентификационная информация должна быть защищена от несанкционированного доступа;

3) доверенная вычислительная база должна поддерживать область для собственного выполнения, защищенную 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.

Примеры продуктов: некоторые старые версии UNIX , IBM RACF.

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.

Примеры продуктов: практически все ныне распростаненные ОС и БД -

Windows NT (а значит сюда можно отнести и все его потомки вплоть до Vista), ещё сюда бы попали все современные UNIX-системы, так же DEC VMS, IBM OS/400, Novell NetWare 4.11, Oracle 7, DG AOS/VS II.

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 путем 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.

Примеры продуктов: сюда относятся гораздо более специализированные ОСи - HP-UX BLS, Cray Research Trusted Unicos 8.0, Digital SEVMS, Harris CS/SX, SGI Trusted IRIX.

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 определенные, 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 ее 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.

Примеры продуктов: Honeywell Multics (знаменитый предок UNIX),

Cryptek VSLAN, Trusted XENIX.

Класс B3.

(в дополнение к B2):

1) для произвольного управления доступом должны обязательно использоваться списки управления доступом с указанием разрешенных 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 определенной 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.

Примеры продуктов: единственная система -

Getronics/Wang Federal XTS-300.

Уровень А.

Носит название - верифицируемая безопасность.

Класс А1.

(в дополнение к В3):

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(Life Cycle) и все компоненты системы, имеющие отношение к обеспечению безопасности.

4) должно быть описано соответствие между формальными спецификациями верхнего уровня и исходными текстами.

Примеры продуктов: Boeing MLS LAN (для создания надежных самолетов нужна надежная сеть), Gemini Trusted Network Processor, Honeywell SCOMP.

Далее приведена краткая таблица описывающая требования предъявляемые к каждому классу.

		A1	B3	B2	B1	C2	C1
	Добровольный контроль доступа	✓	+	✓	✓	+	+
	Повторное использование объектов	✓	✓	✓	✓	+	×
	Метки	✓	✓	+	+	×	×
	Целостность меток	✓	✓	✓	+	×	×
	Экспорт помеченных данных	✓	✓	✓	+	×	×
	Экспорт на многоуровневые устр-ва	✓	✓	✓	+	×	×
	Экспорт на одноуровневые устр-ва	✓	✓	✓	+	×	×
	Пометка при печатном выводе	✓	✓	✓	+	×	×
	Принудительный контроль доступа	✓	✓	+	+	×	×
	Уровень допуска субъектов	✓	✓	+	×	×	×
	Метки устройств	✓	✓	+	×	×	×
	Идентификация и аутентификация	✓	✓	✓	+	+	+
	Аудит	✓	+	+	+	+	×
	Доверенный канал взаимодействия	✓	+	+	×	×	×
	Архитектура системы	✓	+	+	+	+	+
	Целостность системы	✓	✓	✓	✓	✓	+
	Тестирование безопасности	+	+	+	+	+	+
	Спецификация и верификация арх-ры	+	+	+	+	×	×
	Анализ на неявные каналы [утечек]	+	+	+	×	×	×
	Система средств поддержки	✓	+	+	×	×	×
	Система конфигурационного управл.	+	✓	+	×	×	×
	Доверенное восстановление	✓	+	×	×	×	×
	Доверенное распространение	+	×	×	×	×	×
	Справочник по функциям безопасности	✓	✓	✓	✓	✓	+
	Справочник по администрированию	✓	+	+	+	+	+
	Документация по тестированию	+	✓	+	✓	✓	+
	Документация по архитектуре	+	+	+	+	✓	+
		A1	B3	B2	B1	C2	C1

Легенда:

 - Дополнительных требований нет,

 - Дополнительные требования,

 - Никаких требований не предъявлено .

Дополнения.

Помимо описания вышеперечисленных классов в Оранжевой книге присутствуют руководства по поиску тайных каналов, руководство по настройке принудительного контроля доступа и руководство по тестированию безопасности.

Интересны например требования, предъявляемые к команде тестирования безопасности систем уровня А: по крайней мере 1 бакалавр по компьютерным технологиям и 2 магистра той же области, далее один человек знающий «железо» ЭВМ на уровне сугубо технической документации разработчика + один человек уровня написания драйверов под тестируемую систему + человек, уже тестировавший системы этого уровня.

Вот насколько важна в данном случае компетентность специалистов!

Ну и самое главное — то, что в самом документе описывается процесс взаимодействия независимых производителей коммерческих продуктов и гос. организаций по оценке безопасности этих продуктов.

Благодаря этому TCSEC превратился в воистину международный стандарт надёжности и безопасности.

Некоторые комментарии.

Как известно, сегодня большая часть серверов Интернета сегодня работает под управлением UNIX-систем (преимущественно Linux). Хотя формально подавляющее большинство их относится к классу C2 (далеко не самому высокому), нельзя называть их небезопасными. Просто дело в том, что серверы являются одноуровневыми системами, где уровни секретности данных пользователей одинаковы. Сложные модели меток и принудительного доступа не повысят их надёжности, но заметно усложнят настройку и управление.

Вдобавок, системы, достигшие уровней B и даже A являются клонами UNIX, с существенно доработанной моделью безопасности.

Существуют реализации моделей принудительного доступа и для свободных операционных систем таких как Linux и FreeBSD — SELinux и TrustedBSD соответственно. Это позволяет существенно усилить их безопасность.

Современные стандарты.

Под влиянием TCSEC в Европе также были созданы национальные стандарты оценки информационных продуктов. Среди них особо стоит отметить Information Technology Security Evaluation Criteria (ITSEC), принятый в Германии, Нидерландах, Англии, Франции и большей части Европы в 1991 году.

В нем и последовавшим за ним Common Criteria (признанным международным в 2000-х годах) к оцениваемым системам не предъявляется никаких изначальных требований, благодаря чему достигается максимальная универсальность проверки. Обратная сторона медали состоит в том,что фактически только сам разработчик предъявляет документ, где четко и однозначно описывает все функции и аспекты безопасности, которые он готов выполнить в своем продукте. А комитет по оценке проверяет лишь то, насколько качественно реализовано заявленная функциональность в заявленных разработчиком условиях тестирования продукта.

Поэтому например в Windows 2000, получившем EAL4+ в 2002 (4 уровень из 7 возможных уровней стандарта CC), найдено огромное число уязвимостей, но результат оценки не был пересмотрен.

Главными недостатками государственных оценок информационной безопасности коммерческих продуктов были и остаются — их высокая стоимость (+цена простоя в разработке,пока продукт проходит оценку), медленность (продукт может просто устареть пока проходит проверку), а главное — всегда некоторая ограниченность и неполноценность, как упоминалось выше. Модель оценки «сверху» все менее вписывается в современную IT-индустрию.

Но тем не менее, сфера компьютерной безопасности не стоит на месте — появляются новые технологии, решения, идеи. Огромный идейный потенциал Оранжевой книги остается всё ещё в силе и, вполне вероятно, будет востребован в новом цифровом веке.