**ОРАНЖЕВАЯ КНИГА**

Критерии безопасности компьютерных систем министерства обороны США или стандарт TCSEC, получившие название «Оранжевая книга», ориентированы на обеспечение безопасности информации в компьютерных системах. При этом понятие «обеспечение безопасности информации» основывается на следующем предположении: компьютерная система является безопасной, если она обеспечивает контроль за доступом к информации так, что только надлежащим образом уполномоченные лица или процессы, функционирующие от их имени, имеют право читать, писать, создавать или уничтожать информацию.

Критерии безопасности, изложенные в «Оранжевой книге», ориентированы в основном на разработку и сертификацию многопользовательских операционных систем и требуют определенной интерпретации для применения в других областях, например для баз данных и сетей.

«Критерии безопасности компьютерных систем» (Trusted Computer System Evalualion Сriteria) были разработаны и опубликованы Министерством обороны США в 1983 году с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному программному и информационному обеспечению компьютерных систем и выработки методики и технологии анализа степени поддержки политики безопасности в компьютерных системах в основном военного назначения.

Без преувеличения можно утверждать, что в «Оранжевой книге» заложен понятийный базис информационной безопасности. Достаточно лишь перечислить содержащиеся в нем понятия: безопасная и доверенная системы; монитор обращений; ядро и периметр безопасности; критерии (требования), политика, уровни и классы безопасности.

**Функциональные требования безопасности**

Предложенные в этом документе концепции защиты и набор функциональных требований послужили основой для формирования всех появившихся впоследствии стандартов безопасности.

В "Оранжевой книге" предложены три категории требований безопасности – политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены непосредственно на обеспечение безопасности информации, а два последних – на качество самих средств защиты. Рассмотрим эти требования подробнее.

Требование 1. Политика безопасности. Система должна поддерживать точно определенную политику безопасности. Возможность осуществления субъектами доступа к объектам должна определяться на основании их идентификации и набора правил управления доступом. Там, где необходимо, должна использоваться политика нормативного управления доступом, позволяющая эффективно реализовать разграничение доступа к категорированной информации (информации, отмеченной грифом секретности – типа "секретно", "сов.секретно" и т.д.).

Требование 2. Метки. С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа. Для реализации нормативного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объекта и/или режимы доступа к этому объекту.

Требование 3. Идентификация и аутентификация. Все субъекты должен 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.

Требование 4. 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 защищенном протоколе. Система регистрации должна осуществлять анализ общего потока событий и выде­лять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективности его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

Требование 5. Контроль корректности функционирования средств защиты. Средства защиты должны содержать независимые аппаратные или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности идентификацию и аутентификацию, регистрацию и учет, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

Требование 6. Непрерывность защиты. Все средства защиты (в т.ч. и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одним из ключевых аспектов формального доказательства безопасности системы.

Рассматриваемые далее критерии безопасности компьютерных систем представляют собой конкретизацию данных обобщенных требований. Базовые требования к безопасности служат основой для критериев, образующих единую шкалу оценки безопасности компьютерных систем, определяющую семь классов безопасности.

**Группы безопасности компьютерных систем**

"Оранжевая книга" предусматривает четыре группы критериев, которые соответствуют различной степени защищенности: от минимальной (группа D) до формально доказанной (группа А). Каждая группа включает один или несколько классов. Группы D и А содержат по одному классу (классы D и А соответственно), группа С – классы Cl, C2, а группа В – Bl, B2, ВЗ, характеризующиеся различными наборами требований безопасности. Уровень безопасности возрастает при движении к группе А, а внутри группы – с возрастанием номера класса.

1. Группа D. Минимальная защита.
   1. Класс D. Минимальная защита. К этому классу относятся все системы, которые не удовлетворяют требованиям других классов.
2. Группа С. Дискреционная защита. Данная характеризуется наличием произвольного управления доступом и регистрацией действий субъектов.
   1. Класс *С1.* Дискреционная защита. Системы этого класса удовлетворяют требованиям обеспечения разделения пользователей и информации и включают средства контроля и управления доступом, позволяющие задавать ограничения для индивидуальных пользователей, что дает им возможность защищать свою приватную информацию от других пользователей. Класс С1 рассчитан на многопользовательские системы, в которых осуществляется совместная обработка данных одного уровня секретности.
   2. Класс С2, Управление доступом. Системы этого класса осуществляют более избирательное управление доступом, чем системы класса С1, с помощью применения средств индивидуального контроля за действиями пользователей, регистрацией, учетом событий и выделением ресурсов.
3. Группа В. Мандатная защита. Основные требования этой группы – нормативное управление доступом с использованием меток безопасности, поддержка модели и политики безопасности, а также наличие спецификаций на функции ТСВ. Для систем этой группы монитор взаимодействий должен контролировать все события в системе.
   1. Класс В1. Защита с применением меток безопасности. Системы класса В1 должны соответствовать всем требованиям, предъявляемым к системам класса С2, и, кроме того, должны поддерживать определенную неформально модель безопасности, маркировку данных и нормативное управление доступом. При экспорте из системы информация должна подвергаться маркировке. Обнаруженные в процессе тестирования недостатки, должны быть устранены.
   2. Класс В2. Структурированная защита. Для соответствия классу В2 ТСВ система должна поддерживать формально определенную и четко документированную модель безопасности, предусматривающую произвольное и нормативное управление доступом, которое распространяется по сравнению с системами класса В1 на все субъекты. Кроме того, должен осуществляться контроль скрытых каналов утечки информации. В структуре ТСВ должны быть выделены элементы, критичные с точки зрения безопасности. Интерфейс ТСВ должен быть четко определен, а ее архитектура и реализация должны быть выполнены с учетом возможности проведения тестовых испытаний. По сравнению с классом В1 должны быть усилены средства аутентификации. Управление безопасностью осуществляется администраторами системы. Должны быть предусмотрены средства управления конфигурацией.
   3. Класс ВЗ. Домены безопасности. Для соответствия этому классу ТСВ система должна поддерживать монитор взаимодействий, который контролирует все типы доступа субъектов к объектам, который невозможно обойти. Кроме того, ТСВ должна быть структурирована с целью исключения из нее подсистем, не отвечающих за реализацию функций защиты, и быть достаточно компактной для эффективного тестирования и анализа. В ходе разработки и реализации ТСВ должны применяться методы и средства, направленные на минимизацию ее сложности. Средства аудита должны включать механизмы оповещения администратора при возникновении событий, имеющих значение для безопасности системы. Требуется наличие средств восстановления работоспособности системы.
4. Группа А. Верифицированная защита. Данная группа характеризуется применением формальных методов верификации корректности работы механизмов управления доступом (произвольного и нормативного). Требуется дополнительная документация, демонстрирующая, что архитектура и реализация ТСВ отвечают требованиям безопасности.
   1. Класс А1. Формальная верификация. Системы класса А1 функционально эквивалентны системам класса ВЗ, и к ним не предъявляется никаких дополнительных функциональных требований. В отличие от систем класса ВЗ в ходе разработки должны применяться формальные методы верификации, что позволяет с высокой уверенностью получить корректную реализацию функций защиты. Процесс доказательства адекватности реализации начинается на ранней стадии разработки с построения формальной модели политики безопасности и спецификаций высокого уровня. Для обеспечения методов верификации системы класса А1 должны содержать более мощные средства управления конфигурацией и защищенную процедуру дистрибуции.

Приведенные классы безопасности надолго определили основные концепции безопасности и ход развития средств защиты.

**ЕВРОПЕЙСКИЕ КРИТЕРИИ**

После выхода «Оранжевой книги» страны Европы разработали согласованные «Критерии безопасности информационных технологий». (Information Technology Security Evaluation Criteria). Основные положения обсуждаются на основе документа, версия 1.2 которого была опубликована в 1991 году. Страны, участвующие в разработке этого документа – Франция, Германия, Нидерланды и Великобритания.

Рассматриваемой в данном документе понятие безопасности информационной технологии связано не только с защитой конфиденциальности обрабатываемой информации, но и возможностью обеспечения её целостности и доступности.

Второе отличие Европейских критериев от «Оранжевой книги» состоит в том, что они не задают заранее определенную шкалу требований к механизмам защиты. Набор функциональных требований к механизмам обеспечения безопасности может задаваться заказчиком. Целью процесса сертификации в таком случае является определение уровня доверия к реализованным средствам защиты. Для этого в Европейских критериях впервые вводится понятие адекватность (assurance) средств защиты.

Понятие адекватности включает в себя два аспекта:

* эффективность средств защиты, которая определяется соответствием между задачами, поставленными перед средствами безопасности, и реализованным набором функций защиты – их функциональной политикой и согласованностью, простотой использования, а также возможными последствиями использования злоумышленниками 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. Согласно Европейским критериям, мощность можно считать базовой, если механизм защиты способен противостоять отдельным случайным атакам. Мощность можно считать средней, если механизм может противостоять злоумышленникам с ограниченными ресурсами и возможностями. Мощность можно считать высокой, если есть уверенность, что механизм может быть преодолен только высококвалифицированным злоумышленником, возможности и ресурсы которого выходят за пределы разумного.
* корректность средств защиты, которая определяет правильность средств защиты и надежность реализации функций безопасности. При проверке корректности анализируется весь жизненный цикл объекта оценки – от проектирования до эксплуатации и сопровождения.

Корректность в оценке адекватности средств защиты учитывает правильность и надежность реализации функций и механизмов безопасности.

Общая оценка уровня безопасности системы складывается из функциональной мощности средств защиты и уровня адекватности их реализации. При этом Европейские критерии уделяют значительно больше внимания адекватности средств защиты, чем функциональным требованиям.

«Европейские критерии» рассматривают следующие задачи средств информационной безопасности:

* защита информации от несанкционированного доступа с целью обеспечения конфиденциальности;
* обеспечение целостности информации: защита информации от несанкционированной модификации или уничтожения;
* обеспечение работоспособности систем с помощью противодействия угрозам отказа в доступности.

Общая оценка безопасности системы определяется функциональной мощностью средств защиты и уровнем адекватности их реализации.

**Функциональные критерии**

В «Европейских критериях» средства, обеспечивающие информационную безопасность, рассматриваются на трех уровнях детализации:

* на первом уровне рассматриваются цели, в соответствии с которыми разрабатываются средства защиты;
* на втором уровне разрабатываются спецификации функций защиты;
* на третьем уровне – реализуются их механизмы.

Спецификации функций защиты должны выполняться в соответствии со следующими требованиями:

* идентификации и аутентификации;
* управление доступом;
* подотчетность;
* аудит;
* повторное использование объектов;
* целостность информации;
* надежность обслуживания;
* безопасность обмена данными.

Большинство из перечисленных требований совпадают с аналогичными требованиями «Оранжевой книги». Поэтому далее будут рассмотрены только специфичные для «Европейских критериев» моменты.

Требования безопасности обмена данными регламентируют работу средств, которые обеспечивают безопасность данных, передаваемых по каналам связи, и включают следующие разделы:

* аутентификация;
* управление доступом;
* конфиденциальность данных;
* целостность данных;
* невозможность отказаться от совершенных действий.

Набор функций безопасности может специфицироваться с использованием ссылок на заранее определенные классы – шаблоны. В «Европейских критериях» таких классов десять.

Классы F-C1, F-C2, F-B1, F-B2, F-B3 соответствуют классам безопасности «Оранжевой книги» с аналогичными обозначениями.

* + 1. Класс F-IN предназначен для систем с высоким требованием целостности, что типично для систем управления базами данных. Его описание основано на концепции «ролей», соответствующих видам деятельности пользователей, и предоставление доступа к определенным объектам только посредством доверенных процессов. При этом должны различаться следующие виды доступа: чтение, запись, добавление, удаление, создание, переименование и выполнение объектов.
    2. Класс F-AV характеризуется повышенными требованиями к работоспособности. Это существенно, например, для систем управления технологическими процессами. В требованиях этого класса указывается, что восстановление системы после отказа отдельной аппаратной компьютерной системы должно происходить таким образом, чтобы все критически важные функции постоянно оставались доступными. В таком же режиме должна и происходить и замена компонентов системы. Независимо от уровня загрузки должно гарантироваться определенное максимальное время реакции системы на внешнее событие.
    3. Класс F-DI ориентирован на распределение системами обработки информации. Перед началом обмена и при получении данных стороны должны иметь возможность провести идентификацию участников взаимодействия и проверить ее подлинность. Должны использоваться средства контроля и исправления ошибок. В частности, при пересылке данных должны обнаруживаться все случайные или намеренные искажения адресной и пользовательской информации. Знание алгоритмов обнаружения искажений не должно позволять злоумышленнику производить нелегальную модификацию передаваемых данных. Должны обнаруживаться попытки повторной передачи сообщений.
    4. Класс – F-DC уделяет особое внимание требованиям к конфиденциальности, передаваемой информации. Информация по каналам связи должна передаваться только в зашифрованном виде. Ключи шифрования должны быть защищены от несанкционированного доступа.
    5. Класс F-DX предъявляет повышенные требования и к целостности, и к конфиденциальности информации. Его можно рассматривать как функциональное объединение классов F-DI и F-DC с дополнительными возможностями шифрования и защиты от анализа трафика. Должен быть ограничен доступ к ранее переданной информации.

**Критерии адекватности**

В «Европейских критериях» больше внимания уделяется адекватности. При проверке адекватности анализируется весь жизненный цикл компьютерной системы – от начальной фазы проектирования до эксплуатации и управления.

Определено семь уровней адекватности от ЕО до E6 (в порядке возрастания):

* + 1. Уровень ЕО: определяет минимальную адекватность.
    2. Уровень Е1: анализируется общая архитектура системы, а адекватность средств защиты подтверждается функциональным тестированием.
    3. Уровень Е2: осуществляется более тщательный анализ структуры системы и адекватности средств защиты.
    4. Уровень Е3: к анализу привлекаются исходные тексты программ и схемы аппаратного обеспечения.
    5. Жизненный цикл компьютерной системы – от начальной фазы проектирования до эксплуатации и управления.
    6. Уровни Е4, Е5: характеризуются более тщательным анализом исходных текстов программ и схем аппаратного обеспечения.
    7. Уровень Е6: требует формального описания функций безопасности, общей архитектуры, а также политики безопасности.

В "Европейских критериях" определены три уровня безопасности:

* базовый – безопасность считается базовой, если средства защиты способны противостоять отдельным случайным атакам;
* средний – безопасность считается средней, если средства защиты способны противостоять атакам злоумышленников, обладающими ограниченными ресурсами и возможностями;
* высокий – безопасность считается высокой, если, средства защиты могут быть преодолены только злоумышленником с высокой квалификацией, набор возможностей и ресурсов которого выходит за рамки возможного.

**СПАВНЕНИЕ ПО КРИТЕРИЯМ**

Главная задача стандартов информационной безопасности — со­гласовать позиции и цели производителей, потребителей и аналити­ков-классификаторов в процессе создания и эксплуатации продуктов информационных технологий. Каждая из перечисленных категорий специалистов оценивает стандарты и содержащиеся в них требования и критерии по своим собственным параметрам.

В качестве обобщенных показателей, характеризующих стандар­ты информационной безопасности и имеющих значение для всех трех сторон, предлагается использовать универсальность, гибкость, гарантированность, реализуемость и актуальность.

***Универсальность****.* «Оранжевая книга» предназначалась для сис­тем военного времени, ее адаптация для распределенных систем и баз данных потребовала разработки дополнительных документов.

В «Европейские критерии» вошли распределенные системы, се­ти, системы телекоммуникаций и СУБД, но в данном стандарте по-прежнему явным образом оговаривается архитектура и назначение систем, к которым он может быть применен, и никак не регламен­тируется среда их эксплуатации.

***Гибкость****.* Требования «Оранжевой книги» оказались слишком абстрактными для непосредственного применения во многих случа­ях, что потребовало их дополнения.

«Европейские критерии» предусмотрели специальные уровни и требования, рассчитанные на типовые системы (СУБД, телекоммуни­кации и т.д.).

***Гарантированность****.* «Оранжевая книга» предусматривала обя­зательное применение формальных методов верификации только при создании систем высшего класса защищенности (класс А). В 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. Среди архитектурных решений, предусматриваемых "Оранжевой книгой", упомянем следующие:

* Деление аппаратных и системных функций по уровням привилегированности и контроль обмена информацией между уровнями.
* Защита различных процессов от взаимного влияния за счет механизма виртуальной памяти.
* Наличие средств управления доступом.
* Структурированность системы, явное выделение надежной вычислительной базы, обеспечение компактности этой базы.
* Следование принципу минимизации привилегий — каждому компоненту дается ровно столько привилегий, сколько необходимо для выполнения им своих функций.
* Сегментация (в частности, сегментация адресного пространства процессов) как средство повышения надежности компонентов.

В «Европейских критериях» появляется специальный раздел требований — требования адекватности, которые были рассмотрены выше.

***Реализуемость****.* Плохие показатели реализуемости говорят о практической бесполезности стандарта, поэтому все документы отве­чают этому показателю в достаточной или высокой степени.

***Актуальность****.* «Оранжевая книга» содержит требования, в ос­новном направленные на противодействие угрозам конфиденци­альности, что объясняется ее ориентированностью на системы во­енного назначения.

«Европейские критерии» находятся примерно на том же уровне, хотя и уделяют угрозам целостности гораздо больше внимания.

ВЫВОДЫ

«Критерии безопасности компьютерных систем» Министерства Обороны США представляют собой первую попытку создать единый стандарт безопасности, рассчитанный на проектировщиков, разработчиков, потребителей и специалистов по сертификации систем безопасности компьютерных систем. В свое время этот документ явился значительным шагом в области безопасности информационных технологий и послужил отправной точкой для многочисленных исследований и разработок. Основной отличительной чертой этого документа является его ориентация на системы военного применения, причем в основном на операционные системы. Это предопределено доминирование требований, направленных на обеспечение конфиденциальности обрабатываемой информации, и исключение возможностей ее разглашения. Большое внимание уделено меткам конфиденциальности (грифом секретности) и правилам экспорта секретной информации.

Требования по гарантированию политики безопасности отражены поверхностно, соответствующий раздел по существу ограничивается требованиями контроля целостности средств защиты и поддержанию их работоспособности, чего явно недостаточно.

"Оранжевая книга" послужила основой для разработки всех остальных стандартов информационной безопасности, в том числе Российских стандартов, принятых Гостехкомиссией, и современных международных критериев безопасности информационных технологий, и до сих пор используется в США в качестве руководящего документа при сертификации компьютерных систем обработки информации.

«Европейские критерии безопасности информационных технологий» оказали существенное влияние на стандарты безопасности и методику сертификации.

Главное достижение этого документа – введение понятия адекватности средств защиты и определение отдельной шкалы (уровней адекватности) для критериев адекватности.

Необходимо отметить, что «Европейские критерии» тесно связаны с «Оранжевой книгой», что делает их не вполне самостоятельным документом.