# **ВВЕДЕНИЕ**

В настоящее время имеет большое значение система стандартов и иных нормативных документов, используемых в большинстве развитых стран и устанавливающих требования к защищенности информации в компьютерных системах. В большинстве случаев эти требования задаются перечнем механизмов защиты, которые необходимо иметь в КС для того, чтобы она соответствовала определенному классу защиты.

Комплексный документ впервые появился в США в 1983 г. были опубликованы «Критерии оценки безопасности компьютерных систем» (Trusted Computer System Evaluation Criteria, TCSEC), разработанные министерством обороны США. За данным документом закрепилось неформальное название «Оранжевая книга».

Позже в 1991 году страны Европы (Франция, Германия, Великобритания и Голландия) приняли согласованный документ под названием Критерии безопасности информационных технологий «Information Technology Security Evaluation Criteria, ITSEC»).

# **«ОРАНЖЕВАЯ КНИГА»**

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 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.

В «Оранжевой книге» заложен понятийный базис информационной безопасности.

* 1. Функциональные требования безопасности

В "Оранжевой книге" предложены три категории требований безопасности – политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности.

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.

Требование 2. Метки. С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа.

Требование 3. Идентификация и аутентификация. Все субъекты должен иметь уникальные идентификаторы.

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.

Требование 5. Контроль корректности функционирования средств защиты. Средства защиты должны содержать независимые аппаратные или программные компоненты, обеспечивающие работоспособность функций 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.

* 1. Группы безопасности компьютерных систем

Критерии TCSEC разработаны на основе принципа достоверной вычислительной базы (ТСВ). В "Оранжевой книге" ТСВ определяется как "совокупность механизмов защиты, входящих в вычислительную систему и включающих в себя аппаратные, программно-аппаратные и программные средства, сочетание которых и обеспечивает реализацию стратегии защиты".

"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 C1, C2, а группа В – B1, 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.
   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.
   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.
   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.
   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.
4. Группа А. Верифицированная защита. Данная группа характеризуется применением формальных методов верификации корректности работы механизмов управления доступом (произвольного и нормативного).
   1. Класс А1. Формальная верификация. Системы класса А1 функционально эквивалентны системам класса ВЗ, и к ним не предъявляется никаких дополнительных функциональных требований.

# **ЕВРОПЕЙСКИЕ КРИТЕРИИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

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.

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

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.

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.
* корректность средств защиты, которая определяет правильность средств защиты и надежность реализации функций безопасности.

Общая оценка уровня безопасности системы складывается из функциональной мощности средств защиты и уровня адекватности их реализации.

«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.
  1. 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».

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.

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
    2. Класс F-AV характеризуется повышенными требованиями к работоспособности.
    3. Класс F-DI ориентирован на распределение системами обработки информации.
    4. Класс – F-DC уделяет особое внимание требованиям к конфиденциальности, передаваемой информации
    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.
  1. Критерии адекватности

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. Уровни Е4, Е5: характеризуются более тщательным анализом исходных текстов программ и схем аппаратного обеспечения.
    6. 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.

# **СРАВНЕНИЕ КРИТЕРИЕВ ПО ОБОБЩЕННЫМ ПОКАЗАТЕЛЯМ**

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.

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.

# **ЗАКЛЮЧЕНИЕ**

«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.

«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.