**Обзор международных стандартов защиты информации**

## Роль стандартов ИБ

С развитием ИТ (инфо- технологий) появилась необходимость стандартизации требований в области защиты информации.

*Главная задача стандартов ИБ* – создать основу для взаимодействия между производителями, потребителями и специалистами по сертификации. Каждая из этих групп имеет свои интересы и свои взгляды на проблему ИБ.

* *Потребители* заинтересованы в методике, позволяющей обоснованно выбрать продукт, отвечающий их нуждам и решающий их проблемы, для чего им необходима шкала оценки безопасности. Потребители также нуждаются в инструменте, с помощью которого они могли бы формулировать свои требования производителям. При этом потребителей интересуют исключительно характеристики и свойства конечного продукта, а не методы и средства их достижения. К сожалению, многие потребители не понимают, что требования безопасности обязательно противоречат функциональным требованиям (удобству работы, быстродействию и т. д.), накладывают ограничения на совместимость и, как правило, вынуждают отказаться от широко распространенных и поэтому незащищенных прикладных программных средств.
* *Производители* нуждаются в стандартах как средстве сравнения возможностей своих продуктов, в применении процедуры сертификации как механизма объективной оценки их свойств, а также в стандартизации определенного набора требований безопасности, который мог бы ограничить фантазию заказчика конкретного продукта и заставить его выбирать требования из этого набора. С точки зрения производителя требования безопасности должны быть максимально конкретными и регламентировать необходимость применения тех или иных средств, механизмов, алгоритмов и т. д. Кроме того, требования не должны противоречить существующим парадигмам обработки информации, архитектуре вычислительных систем и технологиям создания информационных продуктов. Однако такой подход также нельзя признать в качестве доминирующего, так как он не учитывает нужд пользователей и пытается подогнать требования защиты под существующие системы и технологии.
* *Эксперты по квалификации* и *специалисты по сертификации*рассматривают стандарты как инструмент, позволяющий им оценить уровень безопасности, обеспечиваемый продуктами ИТ, и предоставить потребителям возможность сделать обоснованный выбор. Эксперты по квалификации находятся в двойственном положении: с одной стороны, они, как и производители, заинтересованы в четких и простых критериях, над которыми не надо ломать голову, как их применить к конкретному продукту, а с другой стороны, они должны дать обоснованный ответ пользователям — удовлетворяет продукт их нужды или нет. Именно они берут ответственность за безопасность продукта, получившего квалификацию, уровень безопасности и прошедшего сертификацию

Таким образом, перед стандартами информационной безопасности стоит непростая задача — **создать эффективный механизм взаимодействия всех сторон**. Причем ущемление потребностей хотя бы одной из них приведет к невозможности взаимопонимания и взаимодействия и, следовательно, не позволит решить общую задачу — создание защищенной системы обработки информации

Наиболее значимыми стандартами ИБ являются «Критерии безопасности компьютерных систем» Министерства обороны США, «Руководящие документы Гостехкомиссии России», «Европейские критерии безопасности информационных технологий», «Федеральные критерии безопасности информационных технологий США», «Канадские критерии безопасности компьютерных систем», «Единые критерии безопасности ИТ».

## Критерии безопасности компьютерных систем министерства обороны США (оранжевая книга)

Критерии безопасности КС (компьютерные системы) получившие неформальное название «Оранжевая книга» были разработаны министерством обороны США в 1983 году с целью определения требований безопасности предъявляемых к аппаратному, программному и специальному обеспечению КС и выработке соответствующей методологии и технологии, анализа степени поддержки, политики безопасности в КС военного назначения

В данном док-те были впервые нормативно определены такие понятия как: политика безопасности, ядро безопасности и т.д., предложенные в этом док-те концепции зашиты и набор функциональных требований послужили основой для формирования всех появившихся в последствии стандартов безопасности.

**Ядро безопасности** – это совокупность аппаратных, программных и специальных компонент вычислительной системы, реализующей ф-ии защиты и обеспечения безопасности.

**Таксономия** – это наука о систематизации и классификации сложно организованных объектов и явлений, имеющий иерархическое строение. Основана на декомпозиции явлений и их поэтапном уточнении свойств объектов.

**Политика безопасности** – это совокупность норм и правил, обеспечивающее эффективную защиту систему обработки информации от заданного множества угроз безопасности.

**Модель безопасности** – формальное представление ПБ

**Дискреционное управление доступом** – это управление доступом, осуществляемое на основании заданного администратором множества разрешённых отношений доступа.

**Мандатное управление доступом** – это управление доступом, основанное на совокупности правил предоставления доступа определённых на множестве атрибутов безопасности субъектов и объектов.

В оранжевой книге предложены 3 критерия безопасности:

1. ПБ;
2. Аудит;
3. Корректность.

В рамках этих критериев сформулированы 6 базовых требований безопасности.

1. ПБ
   * Система должна поддерживать точно определенную ПБ. 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.).
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.
3. 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.
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 или уничтожения.
5. Контроль корректности функционирования средств защиты
   * Средства защиты должны содержать независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает. что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и меткими безопасности, идентификацию и аутентификацию, регистрацию и учет, должны находится под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.
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 КС в целом. Данное требование распространяется на весь жизненный цикл КС. Кроме того, его выполнение является одним из ключевых аспектов формального доказательства безопасности системы.

Приведённые базовые требования к безопасности служат основой для критериев, образующих единую шкалу оценки безопасности КС, определяющую семь классов безопасности.

## Классы 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 D1 и А1 соответственно), группа С – классы C1, C2, а группа В – B1, B2, ВЗ, характеризующиеся различными наборами требований безопасности. Уровень безопасности возрастает при движении от группы D к группе А, а внутри группы – с возрастанием номера класса.

• **Группа D.** «Минимальная защита**»**

• **Группа С**. «Дискреционная защита»

**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.

**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.

• **Группа В**. Мандатная защита

Основные требования этой группы – нормативное управление доступом с использованием мер безопасности, поддержка МБ и ПБ, а также наличия спецификаций на ф-ий TCB (ЯБ).

Для систем этой группы монитор взаимодействий д/контролировать все события в системе.

**Класс B1**. «Защита с применением меток безопасности»

Системы класса B1 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.

**Класс В2.** «Структурированная защита».

Для соответствия классу В2 TCB (ЯБ) системы должны 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 его 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.

**Класс ВЗ**. «Домены безопасности».

Для соответствия этому классу TCP системы должно поддерживать монитор взаимодействий, который контролирует все типы доступа субъектов к объектам и который невозможно обойти. Кроме того, ТСВ должно быть структурировано с целью исключения из него подсистем, не отвечающих за реализацию функции защиты, и быть достаточно компактно для эффективного тестирования и анализа. В ходе разработки и реализации ТСВ должны применяться методы и средства, направленные на минимизацию его сложности. Средства аудита должны включать механизмы оповещения администратора при возникновении событий, имеющих значение для безопасности системы. Требуется наличие средств восстановления работоспособности системы.

• **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.

**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.

Высший класс безопасности, требующий осуществ­ления верификации средств защиты, построен на доказательстве соответствия программного обеспечения его спецификациям с помощью специальных методик, однако это доказательство (очень дорогостоящее, трудоемкое и практически неосуществимое для реальных операционных систем) не подтверждает корректность и адекватность реализации политики безопасности.

Приведённые классы безопасности надолго определили основные концепции безопасности и ход развития средств защиты

## Классы безопасности компьютерных систем

**Группа D.** «Минимальная защита**» -** ну как бы да

**Группа С**. «Дискреционная защита» - произвольное управление доступом

**Класс С1.** «Дискреционная защита». – базовые требования

**Класс С2.** «Управление доступом». – система ответственности пользователя за некорректные или несанкционированные действия

**Группа В**. «Мандатная защита» - принудительное управление доступом

**Класс B1**. «Защита с применением меток безопасности» - маркировка данных

**Класс В2.** «Структурированная защита». – полный контроль каналов информации;

**Класс ВЗ**. «Домены безопасности». – монитор взаимодействий, механизмы оповещения

**Группа А**. «Верифицированная защита» - верифицируемая безопасность.

**Класс А1**. «Формальная верификация». – мощные средства управления конфигурацией и защищенную процедуру дистрибуции.

Группа D

«Минимальная защита»

Группа C

«Дискреционная защита»

Группа B

«Мандатная защита»

Классы безопасности компьютерных систем

Группа A

«Верифицированная защита»

мощные средства управления конфигурацией и защищенную процедуру дистрибуции

монитор взаимодействий, механизмы оповещения

полный контроль каналов информации

Маркировка данных

Группа А1

«Мандатная защита»

Класс B2

«Структурированная защита»

Класс B3

«Домены безопасности»

Класс B1

«Защита с применением меток безопасности»

система ответственности пользователя за некорректные или несанкционированные действия

Класс C2

«Дискреционная защита»

базовые требования

Класс C1

«Дискреционная защита»

«Минимальный минимум»

**Европейские критерии безопасности информационных технологий.**

Проблемы информационной безопасности актуальны не только для Соединенных Штатов. Вслед за выходом «Оранжевой книги» страны Европы совместно разработали общие «Критерии безопасности информационных технологий» («Information Technology Security Evaluation Criteria», далее «Европейские критерии») [16]. Данный обзор основывается на версии 1.2. опубликованной в июне 1991 года от имени соответствующих органов четырех стран: Франции, Германии, Нидерландов и Великобритании.

2.6.1. Основные понятия

«Европейские критерии» рассматривают следующие задачи средств информационной безопасности:

1. Защита информации от несанкционированного доступа с целью обеспечения конфиденциальности;
2. Обеспечение целостности информации посредством защиты от ее несанкционированной модификации или уничтожения;
3. Обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании.

В «Европейских критериях» проводится различие между системами и продуктами.

Система — это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении.

Продукт— это аппаратно-программный «пакет», который можно купить и по-своему усмотрению встроить в ту или иную систему.

Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях.

Угрозы безопасности системы носят вполне конкретный и реальный характер. Относительно угроз продукту можно лишь строить предположения. Разработчик может специфицировать условия, пригодные для функционирования продукта; дело покупателя обеспечить выполнение этих условий.

Из практических соображений важно обеспечить единство критериев оценки продуктов и систем — облегчить и удешевить оценку системы, составленной из ранее сертифицированных продуктов. В этой связи для систем и продуктов вводится единый термин — **объект оценки**.

Для того чтобы удовлетворить требованиям конфиденциальности, целостности и работоспособности, необходимо реализовать соответствующий набор функций безопасности, таких, как идентификация и аутентификация, управление доступом, восстановление после сбоев и т. п. Чтобы средства защиты можно было признать эффективными, требуется определенная степень уверенности в правильности их выбора и надежности функционирования. Для решения этой проблемы в «Европейских критериях» впервые вводится понятие адекватности (assurance) средств защиты.

Для решения этой проблемы в **«Европейских критериях»** впервые вводится **понятие адекватности (assurance) средств защиты**. Общая оценка уровня безопасности системы складывается из функциональной мощности средств защиты и уровня адекватности их реализации.

Большинство требований безопасности совпадает с аналогичными требованиями Оранжевой книги. В «Европейских критериях» определено десять классов безопасности. Классы F-C1, F-C2, F-B1, F-B2, F-B3 соответствуют классам безопасности Оранжевой книги с аналогичными обозначениями.

**Класс F-IN предназначен** для систем с высокими потребностями в обеспечении целостности, что типично для систем управления базами данных.

Его описание основано на концепции «ролей», соответствующих видам деятельности пользователей, и предоставлении доступа к определённым объектам только посредством доверенных процессов. Должны различаться следующие виды доступа: чтение, запись, добавление, удаление, создание, переименование и выполнение объектов.

**Класс F-AV** характеризуется повышенными требованиями к обеспечению работоспособности.

Это существенно, например для систем управления технологическими процессами. В **требованиях** этого класса указывается, что система должна восстанавливаться после отказа отдельного аппаратного компонента таким образом, чтобы все критически важные функции постоянно оставались доступными. В таком же режиме должна происходить и замена компонентов системы. Независимо от уровня загрузки должно гарантироваться определенное время реакции системы на внешние события.

**Класс F-DI** ориентирован на распределенные системы 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 алгоритма обнаружения искажений не должно позволять злоумышленнику производить нелегальную модификацию передаваемых данных. Необходимо обнаруживать попытки повторной передачи ранее переданных сообщений.

**Класс F-DC** уделяет особое внимание требованиями к конфиденциальности передаваемой информации. Информация по каналам связи должна передаваться в зашифрованном виде. Ключи шифрования защищают от несанкционированного доступа.

**Класс F-DX** предъявляет повышенные требования и к целостности и к конфиденциальности информации. Его можно рассматривать как объединение классов F-DI и F-DC с дополнительными возможностями шифрования и защиты от анализа трафика. Следует ограничить доступ к ранее переданной информации, которая в принципе может способствовать проведению криптоанализа.

**Критерии адекватности.**

Адекватность включает в себя два аспекта: эффективность, отражающую соответствие средств безопасности решаемым задачам, и корректность, характеризующую процесс их разработки и функционирования.

**Эффективность** — соответствие между задачами, поставленными перед средствами безопасности, и реализованным набором функций защиты — их функциональной полнотой и согласованностью, простотой использования, а также возможными последствиями использования злоумышленниками слабых мест защиты.

**Корректность** — правильность и надежность реализации функций безопасности.

Европейские критерии определяют **семь уровней адекватности** — от Е0 до Е6. При проверке адекватности анализируется весь жизненный цикл системы — от начальной фазы проектирования до эксплуатации и сопровождения.

**Уровни адекватности от Е1 до Е6** выстроены по нарастанию требований тщательности контроля. Так, на уровне Е1 анализируется лишь общая архитектура системы, а адекватность средств защиты подтверждается функциональным тестированием.

**На уровне ЕЗ** к анализу привлекаются исходные тексты программ и схемы аппаратного обеспечения. **На уровне Е6** требуется формальное описание функций безопасности, общей архитектуры, а также политики безопасности.

В Европейских критериях определены три уровня безопасности — базовый, средний и высокий. Степень безопасности системы определяется самым слабым из критически важных механизмов защиты.

Безопасность считается базовой, если средства защиты способны противостоять отдельным случайным атакам. Безопасность считается средней, если средства защиты способны противостоять злоумышленникам, обладающим ограниченными ресурсами и возможностями. Наконец, безопасность можно считать высокой, если есть уверенность, что средства защиты могут быть преодолены только злоумышленником с высокой квалификацией, набор возможностей и ресурсов которого выходит за рамки возможного.

Итак, **Европейские критерии безопасности информационных технологий**, появившиеся вслед за Оранжевой книгой, оказали существенное влияние на стандарты безопасности и методику сертификации.

Главное **достижение** этого документа — **введение понятия адекватности средств защиты и определение отдельной шкалы для критериев адекватности**. Как уже упоминалось, Европейские критерии придают адекватность средств защиты даже большее значение, чем их функциональности. Этот подход используется во многих появившихся позднее стандартах информационной безопасности.