**"Оранжевая книга"**

Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США *"Критерии оценки доверенных компьютерных систем"*.

Данный труд, называемый чаще всего по цвету обложки "Оранжевой книгой", был впервые опубликован в августе 1983 года. Уже одно его название требует комментария. Речь идет не о безопасных, а о доверенных системах, то есть системах, которым можно оказать определенную степень доверия.

"Оранжевая книга" поясняет понятие безопасной системы, которая "управляет, с помощью соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию".

В "Оранжевой книге" **доверенная система** определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Степень доверия оценивается по двум основным критериям:

* **Политика безопасности (ПБ)** — набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть ПБ. Конкретные средства защиты определяются исходя из политики безопасности. ПБ — это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.
* **Уровень гарантированности** — мера доверия, которая может быть оказана архитектуре и реализации ИС. Это доверие может основываться как на анализе результатов тестирования, так и на проверке общего замысла и реализации ИС или отдельных её компонентов. Уровень гарантированности показывает, насколько корректно работают средства защиты, отвечающие за реализацию политики безопасности. Это пассивный аспект защиты.

При оценке степени доверия безопасности определяющее значение имеет доверенная вычислительная база (ДВБ). ДВБ — это совокупность аппаратных и программных механизмов защиты ИС, отвечающих за выполнение ПБ. Качество ДВБ определяется исключительно её реализацией и корректностью исходных данных. Компоненты вне ДВБ могут не быть доверенными. Границу ДВБ называют **периметром безопасности**. С развитием распределённых систем под периметром безопасности всё чаще понимают границу владений определённой организации. То, что находится внутри владений, считается доверенным, а то, что вне, — нет.

В ОК определяются 4 класса доверия: D, C, B, A. Уровень D соответствует системам, признанным неудовлетворительными. По мере перехода от уровня C к A к системам предъявляются всё более жесткие требования. Уровни C, B и A подразделяются на классы. Всего имеется шесть классов безопасности: C1 (дискреционный или разграничительный уровень безопасности), C2 (защищённый управляемый доступ), B1 (уровень безопасности на основе меток), B2 (структурированная модель защиты), B3 (доменный уровень безопасности), A1 (верифицируемый уровень безопасности). Чтобы в результате процедуры сертификации систему можно было отнести к некоторому классу, её ПБ и уровень гарантированности должны удовлетворять заданным требованиям. Современные версии ОС Windows и Unix, Linux при определённых настройках и дополнениях соответствуют классу безопасности 2.

Класс C1:

* доверенная вычислительная база должна управлять доступом именованных пользователей к именованным объектам;
* пользователи должны идентифицировать себя, прежде чем выполнять какие-либо иные действия, контролируемые доверенной вычислительной базой.
* доверенная вычислительная база должна поддерживать область для собственного выполнения, защищенную от внешних воздействий (в частности, от изменения команд и/или данных) и от попыток слежения за ходом работы;
* защитные механизмы должны быть протестированы на предмет соответствия их поведения системной документации.
* должны быть описаны подход к безопасности, используемый производителем, и применение этого подхода при реализации доверенной вычислительной базы.

Класс C2 (в дополнение к C1):

* права доступа должны гранулироваться с точностью до пользователя.
* при выделении хранимого объекта из пула ресурсов доверенной вычислительной базы необходимо ликвидировать все следы его использования;
* каждый пользователь системы должен уникальным образом идентифицироваться.
* доверенная вычислительная база должна создавать, поддерживать и защищать журнал регистрационной информации, относящейся к доступу к объектам, контролируемым базой;

Класс B1 (в дополнение к C2):

* доверенная вычислительная база должна управлять метками безопасности, ассоциируемыми с каждым субъектом и хранимым объектом;
* доверенная вычислительная база должна обеспечить реализацию принудительного управления доступом всех субъектов ко всем хранимым объектам;
* доверенная вычислительная база должна обеспечивать взаимную изоляцию процессов путем разделения их адресных пространств;

Класс B2 (в дополнение к B1):

* должна быть предусмотрена возможность регистрации событий, связанных с организацией тайных каналов обмена с памятью;
* системный архитектор должен тщательно проанализировать возможности организации тайных каналов обмена с памятью и оценить максимальную пропускную способность каждого выявленного канала;
* должна быть продемонстрирована относительная устойчивость доверенной вычислительной базы к попыткам проникновения;
* модель политики безопасности должна быть формальной.
* тесты должны подтверждать действенность мер по уменьшению пропускной способности тайных каналов передачи информации.

Класс B3 (в дополнение к B2):

* должна быть предусмотрена возможность регистрации появления или накопления событий, несущих угрозу политике безопасности системы.
* доверенная вычислительная база должна быть спроектирована и структурирована таким образом, чтобы использовать полный и концептуально простой защитный механизм с точно определенной семантикой;
* процедура анализа должна быть выполнена для временных тайных каналов;
* должна быть специфицирована роль администратора безопасности.
* должны существовать процедуры и/или механизмы, позволяющие произвести восстановление после сбоя или иного нарушения работы без ослабления защиты;

Класс A1 (в дополнение к B3):

* тестирование должно продемонстрировать, что реализация доверенной вычислительной базы соответствует формальным спецификациям верхнего уровня;
* механизм конфигурационного управления должен распространяться на весь жизненный цикл и все компоненты системы, имеющие отношение к обеспечению безопасности;

**Рекомендации X.800**

Данный документ описывает вопросы ИБ распределённых систем, используемые для их защиты сетевые сервисы (функции) безопасности, а также необходимые для реализации этих функций защитные механизмы.

Выделяют следующие сервисы безопасности и исполняемые ими роли:

**Аутентификация**. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

**Управление доступом**. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

**Конфиденциальность данных**. Обеспечивает защиту от несанкционированного получения информации.

**Целостность данных** подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры - с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

**Неотказуемость** (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки. Побочным продуктом неотказуемости является аутентификация источника данных.

Сетевые механизмы безопасности

Для реализации сервисов (функций) безопасности могут использоваться следующие механизмы и их комбинации:

* *шифрование;*
* *электронная цифровая подпись;*
* *механизмы управления доступом*. Могут располагаться на любой из участвующих в общении сторон или в промежуточной точке;
* *механизмы контроля целостности данных*. В рекомендациях X.800 различаются два аспекта целостности: целостность отдельного сообщения или поля информации и целостность потока сообщений или полей информации. Для проверки целостности потока сообщений (то есть для защиты от кражи, переупорядочивания, дублирования и вставки сообщений) используются порядковые номера, временные штампы, криптографическое связывание или иные аналогичные приемы;
* *механизмы аутентификации*. Согласно рекомендациям X.800, аутентификация может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов, устройств измерения и анализа биометрических характеристик;
* *механизмы дополнения трафика;*
* *механизмы управления маршрутизацией*. Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными;
* *механизмы нотаризации*. Служат для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией. Обычно нотаризация опирается на механизм электронной подписи.

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:

* *администрирование информационной системы в целом;*
* *администрирование сервисов безопасности;*
* *администрирование механизмов безопасности.*