[ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ]

[Институт ИИБС, Кафедра ИСКТ]

[Шумейко Е.В.]

Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт

Основные понятия

Мы приступаем к обзору стандартов и спецификаций двух разных видов:

- оценочных стандартов, направленных на классификацию информационных систем и средств защиты по требованиям безопасности;
- технических спецификаций, регламентирующих различные аспекты *реализации* средств защиты.

Важно отметить, что между этими видами нормативных документов нет глухой стены. Оценочные стандарты выделяют важнейшие, с точки зрения ИБ, аспекты ИС, играя роль архитектурных спецификаций. Другие технические спецификации определяют, как строить ИС предписанной архитектуры.

Основные понятия

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*.

Основные понятия

"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". Очевидно, однако, что абсолютно *безопасных систем* не существует, это абстракция. Есть смысл оценивать лишь *степень доверия*, которое можно оказать той или иной системе.

Основные понятия

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". Обратим внимание, что в рассматриваемых Критериях и безопасность, и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности и целостности (статической). Вопросы доступности "Оранжевая книга" не затрагивает.

Основные понятия

Степень доверия оценивается по двум основным критериям.

1. ***Политика безопасности*** - 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 *политика безопасности*. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. *Политика безопасности* - это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

Основные понятия

Степень доверия оценивается по двум основным критериям.

1. ***Политика безопасности*** - 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 *политика безопасности*. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. *Политика безопасности* - это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

Основные понятия

2. ***Уровень гарантированности*** - мера доверия, которая может быть оказана архитектуре и *реализации* ИС. Доверие безопасности может проистекать как из анализа результатов *тестирования*, так и из проверки (формальной или нет) общего замысла и *реализации* системы в целом и отдельных ее компонентов. *Уровень гарантированности* показывает, насколько корректны механизмы, отвечающие за *реализацию политики безопасности*. Это пассивный аспект защиты.

Основные понятия

Важным средством обеспечения безопасности является механизм *подотчетности* (протоколирования). *Доверенная система* должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть *анализом регистрационной информации*.

Концепция *доверенной вычислительной базы* является центральной при оценке *степени доверия* безопасности.

Доверенная вычислительная база - это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь *политики безопасности*. Качество вычислительной базы определяется исключительно ее *реализацией* и корректностью исходных данных, которые вводит системный администратор.

Основные понятия

Вообще говоря, компоненты вне вычислительной базы могут не быть доверенными, однако это не должно влиять на безопасность системы в целом. В результате, для оценки доверия безопасности ИС достаточно рассмотреть только ее вычислительную базу, которая, как можно надеяться, достаточно компактна.

Основное назначение *доверенной вычислительной базы* - выполнять функции *монитора обращений*, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

Основные понятия

Монитор обращений должен обладать тремя качествами:

1. *Изолированность*. Необходимо предупредить возможность отслеживания работы монитора.
2. *Полнота*. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.
3. *Верифицируемость*. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в *полноте тестирования*.

Реализация монитора обращений называется *ядром безопасности*. *Ядро безопасности* - это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств *монитора обращений*, ядро должно гарантировать собственную неизменность.

Основные понятия

Границу *доверенной вычислительной базы* называют ***периметром безопасности***. Как уже указывалось, компоненты, лежащие вне *периметра безопасности*, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию *"периметр безопасности"* все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне, - нет.

Механизмы безопасности

Согласно "Оранжевой книге", *политика безопасности* должна обязательно включать в себя следующие элементы:

- *произвольное управление доступом*;
- *безопасность повторного использования объектов*;
- *метки безопасности*;
- *принудительное управление доступом*.

Механизмы безопасности

Произвольное управление доступом (называемое иногда дискреционным) - это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.

Механизмы безопасности

Безопасность повторного использования объектов - важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной 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.

Механизмы безопасности

Как мы указывали ранее, современный объектно-ориентированный подход резко сужает область действия данного элемента безопасности, затрудняет его *реализацию*. То же верно и для интеллектуальных устройств, способных буферизовать большие объемы данных.

Для *реализации принудительного управления доступом* с субъектами и объектами ассоциируются *метки безопасности*. Метка субъекта описывает его благонадежность, метка объекта - степень конфиденциальности содержащейся в нем информации.

Механизмы безопасности

Согласно "Оранжевой книге", *метки безопасности* состоят из двух частей - уровня секретности и списка категорий. Уровни секретности образуют упорядоченное множество, категории - неупорядоченное. Назначение последних - описать предметную область, к которой относятся данные.

Принудительное (или мандатное) управление доступом основано на сопоставлении *меток безопасности* субъекта и объекта.

Механизмы безопасности

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. Смысл сформулированного правила понятен - читать можно только то, что положено.

Механизмы безопасности

Субъект может записывать информацию в объект, если *метка безопасности* объекта доминирует над меткой субъекта. В частности, "конфиденциальный" субъект может записывать данные в секретные файлы, но не может - в несекретные (разумеется, должны также выполняться ограничения на набор категорий). Описанный способ управления доступом называется *принудительным*, поскольку он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированы *метки безопасности* субъектов и объектов, оказываются зафиксированными и права доступа.

Механизмы безопасности

Если понимать *политику безопасности* узко, то есть как правила разграничения доступа, то механизм *подотчетности* является дополнением подобной политики. Цель *подотчетности* - в каждый момент времени знать, кто работает в системе и что делает. Средства *подотчетности* делятся на три категории:

- *идентификация* и *аутентификация*;
- *предоставление доверенного пути*;
- *анализ регистрационной информации*.

Механизмы безопасности

Обычный способ *идентификации* - ввод имени пользователя при входе в систему. Стандартное средство проверки подлинности (*аутентификации*) пользователя - пароль.

Доверенный путь связывает пользователя непосредственно с *доверенной вычислительной базой*, минуя другие, потенциально опасные компоненты ИС.

Цель *предоставления доверенного пути* - дать пользователю возможность убедиться в подлинности обслуживающей его системы.

Механизмы безопасности

Анализ регистрационной информации (аудит) имеет дело с действиями (событиями), так или иначе затрагивающими безопасность системы.
Если фиксировать все события, объем регистрационной информации, скорее всего, будет расти слишком быстро, а ее эффективный анализ станет невозможным. "Оранжевая книга" предусматривает наличие средств выборочного протоколирования, как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.

Механизмы безопасности

Переходя к пассивным аспектам защиты, укажем, что в "Оранжевой книге" 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*.

Операционная гарантированность включает в себя проверку следующих элементов:

- архитектура системы;
- целостность системы;
- проверка *тайных каналов передачи информации*;
- доверенное администрирование;
- доверенное *восстановление после сбоев*.

Механизмы безопасности

Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее *реализация* действительно реализуют избранную *политику безопасности*.

Технологическая гарантированность охватывает весь *жизненный цикл ИС*, то есть периоды *проектирования*, *реализации*, *тестирования*, *продажи* и *сопровождения*. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и нелегальные "закладки".

Классы безопасности

"Критерии ..." Министерства обороны США открыли путь к ранжированию информационных систем по *степени доверия* безопасности.

В "Оранжевой книге" определяется четыре уровня доверия - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к системам предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием *степени доверия*.

Классы безопасности

Всего имеется шесть *классов безопасности* - C1, C2, B1, B2, B3, A1. Чтобы в результате процедуры сертификации систему можно было отнести к некоторому классу, ее *политика безопасности* и *уровень гарантированности* должны удовлетворять заданным требованиям, из которых мы упомянем лишь важнейшие.

Классы безопасности

Класс С1:

- *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*. Для *аутентификации* должен использоваться какой-либо защитный механизм, например пароли. Аутентификационная информация должна быть защищена от несанкционированного доступа;

Классы безопасности

- *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;
- должны быть в наличии аппаратные и/или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов *доверенной вычислительной базы*;

Классы безопасности

- защитные механизмы должны быть протестированы на предмет соответствия их поведения системной документации. *Тестирование* должно подтвердить, что у неавторизованного пользователя нет очевидных способов обойти или разрушить средства защиты *доверенной вычислительной базы*;
- должны быть описаны подход к безопасности, используемый производителем, и применение этого подхода при *реализации доверенной вычислительной базы*.

Классы безопасности

Класс С2 (в дополнение к С1):

- права доступа должны гранулироваться с точностью до пользователя. Все объекты должны подвергаться контролю доступа;
- при выделении хранимого объекта из пула ресурсов *доверенной вычислительной базы* необходимо ликвидировать все следы его использования;
- каждый пользователь системы должен уникальным образом идентифицироваться. Каждое регистрируемое действие должно ассоциироваться с конкретным пользователем;

Классы безопасности

- *доверенная вычислительная база* должна создавать, поддерживать и защищать журнал регистрационной информации, относящейся к доступу к объектам, контролируемым базой;
- *тестирование* должно подтвердить отсутствие очевидных недостатков в механизмах изоляции ресурсов и защиты регистрационной информации.

Классы безопасности

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*;

Классы безопасности

- группа специалистов, полностью понимающих *реализацию доверенной вычислительной базы*, должна подвергнуть описание архитектуры, исходные и объектные коды тщательному анализу и *тестированию*;
- должна существовать неформальная или формальная модель *политики безопасности*, поддерживаемой *доверенной вычислительной базой*.

Классы безопасности

Класс B2 (в дополнение к B1):

- снабжаться метками должны все ресурсы системы (например, ПЗУ), прямо или косвенно доступные субъектам;
- к *доверенной вычислительной базе* должен поддерживаться доверенный коммуникационный путь для пользователя, выполняющего операции начальной *идентификации* и *аутентификации*;
- должна быть предусмотрена возможность регистрации событий, связанных с организацией тайных каналов обмена с памятью;
- *доверенная вычислительная база* должна быть внутренне структурирована на хорошо определенные, относительно независимые модули;

Классы безопасности

- 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. Для *доверенной вычислительной базы* должны существовать описательные спецификации верхнего уровня, точно и полно определяющие ее интерфейс;

Классы безопасности

- 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;
- тесты должны подтверждать действенность мер по уменьшению пропускной способности *тайных каналов передачи информации*.

Классы безопасности

Класс B3 (в дополнение к B2):

- для *произвольного управления доступом* должны обязательно использоваться *списки управления доступом* с указанием разрешенных режимов;
- 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;

Классы безопасности

- *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*. Получить права *администратора безопасности* можно только после выполнения явных, протоколируемых действий;

Классы безопасности

- должны существовать процедуры и/или механизмы, позволяющие произвести *восстановление после сбоя* или иного нарушения работы без ослабления защиты;
- должна быть продемонстрирована устойчивость *доверенной вычислительной базы* к попыткам проникновения.

Классы безопасности

Класс А1 (в дополнение к В3):

- *тестирование* должно продемонстрировать, что *реализация доверенной вычислительной базы* соответствует *формальным спецификациям верхнего уровня*;
- помимо описательных, должны быть представлены *формальные спецификации верхнего уровня*. Необходимо использовать современные методы формальной спецификации и *верификации* систем;
- механизм конфигурационного управления должен распространяться на весь *жизненный цикл* и все компоненты системы, имеющие отношение к обеспечению безопасности;

Классы безопасности

- должно быть описано соответствие между *формальными спецификациями верхнего уровня* и исходными текстами.

Такова классификация, введенная в "Оранжевой книге". Коротко ее можно сформулировать так:

- уровень C - *произвольное управление доступом*;
- уровень B - *принудительное управление доступом*;
- уровень A - верифицируемая безопасность.

Классы безопасности

Конечно, в адрес "Критериев ..." можно высказать целый ряд серьезных замечаний (таких, например, как полное игнорирование проблем, возникающих в распределенных системах). Тем не менее, следует подчеркнуть, что публикация "Оранжевой книги" без всякого преувеличения стала эпохальным событием в области информационной безопасности. Появился общепризнанный понятийный базис, без которого даже обсуждение проблем ИБ было бы затруднительным.

Классы безопасности

Отметим, что огромный идейный потенциал "Оранжевой книги" пока во многом остается невостребованным. Прежде всего это касается концепции *технологической гарантированности*, охватывающей весь *жизненный цикл системы* - от выработки спецификаций до фазы эксплуатации. При современной технологии программирования результирующая система не содержит информации, присутствующей в исходных спецификациях, теряется информация о семантике программ. Важность данного обстоятельства мы планируем продемонстрировать далее, в лекции об управлении доступом.

Информационная безопасность распределенных систем. Рекомендации X.800

Сетевые сервисы безопасности

Следуя скорее исторической, чем предметной логике, мы переходим к рассмотрению технической спецификации X.800, появившейся немногим позднее "Оранжевой книги", но весьма полно и глубоко трактующей вопросы информационной безопасности распределенных систем. Рекомендации X.800 - документ довольно обширный. Мы остановимся на специфических сетевых функциях (сервисах) безопасности, а также на необходимых для их *реализации* защитных механизмах.

Сетевые сервисы безопасности

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).

Сетевые сервисы безопасности

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

Конфиденциальность данных. Обеспечивает защиту от несанкционированного получения информации. Отдельно упомянем **конфиденциальность трафика** (это защита информации, которую можно получить, анализируя сетевые потоки данных).

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.

Сетевые сервисы безопасности

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**.

В следующей таблице указаны уровни **эталонной семиуровневой модели** OSI, на которых могут быть реализованы функции безопасности. Отметим, что прикладные процессы, в принципе, могут взять на себя поддержку всех защитных сервисов.

Сетевые сервисы безопасности

Таблица 5.1. Распределение функций безопасности по уровням эталонной семиуровневой модели OSI

Функции безопасности	Уровень						
	1	2	3	4	5	6	7
Аутентификация	-	-	+	+	-	-	+
Управление доступом	-	-	+	+	-	-	+
Конфиденциальность соединения	+	+	+	+	-	+	+
Конфиденциальность вне соединения	-	+	+	+	-	+	+
Избирательная конфиденциальность	-	-	-	-	-	+	+
Конфиденциальность трафика	+	-	+	-	-	-	+
Целостность с восстановлением	-	-	-	+	-	-	+
Целостность без восстановления	-	-	+	+	-	-	+
Избирательная целостность	-	-	-	-	-	-	+
Целостность вне соединения	-	-	+	+	-	-	+
Неотказуемость	-	-	-	-	-	-	+

"+" данный уровень может предоставить функцию безопасности;

"-" данный уровень не подходит для предоставления функции безопасности.

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 *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;

Сетевые механизмы безопасности

- 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 **дополнения трафика**;

Сетевые механизмы безопасности

- 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.

Сетевые механизмы безопасности

- В следующей таблице сведены сервисы (функции) и механизмы безопасности. Таблица показывает, какие механизмы (по отдельности или в комбинации с другими) могут использоваться для *реализации* той или иной функции.

Сетевые механизмы безопасности

Таблица 5.2. Взаимосвязь функций и механизмов безопасности

Функции	Механизмы							
	Шифрование	Электронная подпись	Управление доступом	Целостность	Аутентификация	Дополнение трафика	Управление маршрутизацией	Нотаризация
Аутентификация партнеров	+	+	-	-	+	-	-	-
Аутентификация источника	+	+	-	-	-	-	-	-
Управление доступом	-	-	+	-	-	-	-	-
Конфиденциальность	+	-	+	-	-	-	+	-
Избирательная конфиденциальность	+	-	-	-	-	-	-	-
Конфиденциальность трафика	+	-	-	-	-	+	+	-
Целостность соединения	+	-	-	+	-	-	-	-
Целостность вне соединения	+	+	-	+	-	-	-	-
Неотказуемость	-	+	-	+	-	-	-	+

"+" механизм пригоден для *реализации* данной функции безопасности;

"-" механизм не предназначен для *реализации* данной функции безопасности.

Администрирование средств безопасности

Администрирование средств безопасности включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании.

Примерами могут служить распространение **криптографических ключей**, установка значений параметров защиты, ведение регистрационного журнала и т.п.

Концептуальной основой администрирования является информационная база управления безопасностью. Эта база может не существовать как единое (распределенное) хранилище, но каждая из оконечных систем должна располагать информацией, необходимой для *реализации* избранной *политики безопасности*.

Администрирование средств безопасности

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:
администрирование информационной системы в целом;
администрирование сервисов безопасности;
администрирование механизмов безопасности.
Среди действий, относящихся к ИС в целом, отметим обеспечение актуальности *политики безопасности*, взаимодействие с другими административными службами, **реагирование** на происходящие события, **аудит** и **безопасное восстановление**.

Администрирование средств безопасности

Администрирование сервисов безопасности включает в себя определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование механизмов для *реализации* сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Обязанности администратора механизмов безопасности определяются перечнем задействованных механизмов. Типичный список таков:

- **управление ключами (генерация и распределение)**;

Администрирование средств безопасности

- **управление шифрованием** (установка и синхронизация криптографических параметров). К управлению шифрованием можно отнести и администрирование механизмов электронной подписи. Управление целостностью, если оно обеспечивается криптографическими средствами, также тяготеет к данному направлению;
- администрирование управления доступом (распределение информации, необходимой для управления - паролей, списков доступа и т.п.);
- управление *аутентификацией* (распределение информации, необходимой для *аутентификации* - паролей, ключей и т.п.);

Администрирование средств безопасности

- управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений - частоту отправки, размер и т. п.);
- управление маршрутизацией (выделение доверенных путей);
- управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

Мы видим, что администрирование средств безопасности в распределенной ИС имеет много особенностей по сравнению с централизованными системами.

Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

Основные понятия

Мы возвращаемся к теме оценочных стандартов, приступая к рассмотрению самого полного и современного среди них - "Критериев оценки безопасности информационных технологий" (издан 1 декабря 1999 года). Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба.

По историческим причинам данный стандарт часто называют "Общими критериями" (или даже ОК). Мы также будем использовать это сокращение.

Основные понятия

"Общие критерии" на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. В отличие от "Оранжевой книги", ОК не содержат предопределенных *"классов безопасности"*. Такие классы можно строить, исходя из **требований безопасности**, существующих для конкретной организации и/или конкретной информационной системы.

Основные понятия

С программистской точки зрения ОК можно считать набором библиотек, помогающих писать содержательные "программы" - **задания по безопасности**, типовые **профили защиты** и т.п. Программисты знают, насколько хорошая библиотека упрощает разработку программ, повышает их качество. Без библиотек, "с нуля", программы не пишут уже очень давно; оценка безопасности тоже вышла на сопоставимый уровень сложности, и "Общие критерии" предоставили соответствующий инструментарий.

Основные понятия

Важно отметить, что **требования могут быть параметризованы**, как и полагается библиотечным функциям.

Как и "Оранжевая книга", ОК содержат два основных вида **требований** безопасности:

- **функциональные**, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;
- **требования доверия**, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Основные понятия

Требования безопасности предъявляются, а их выполнение проверяется для определенного **объекта оценки** - аппаратно-программного продукта или информационной системы.

Очень важно, что безопасность в ОК рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

- определение назначения, условий применения, целей и требований безопасности;
- *проектирование* и разработка;
- испытания, оценка и сертификация;
- внедрение и эксплуатация.

Основные понятия

В ОК объект оценки рассматривается в контексте **среды безопасности**, которая характеризуется определенными условиями и угрозами.

В свою очередь, угрозы характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Основные понятия

Уязвимые места могут возникать из-за недостатка в:

- требованиях безопасности;
- *проектировании*;
- эксплуатации.

Слабые места по возможности следует устранить, минимизировать или хотя бы постараться ограничить возможный ущерб от их преднамеренного использования или случайной активизации.

Основные понятия

С точки зрения технологии программирования в ОК использован устаревший библиотечный (не объектный) подход. Чтобы, тем не менее, структурировать пространство требований, в "Общих критериях" введена иерархия **класс-семейство-компонент-элемент**.

Классы определяют наиболее общую, "предметную" группировку требований (например, функциональные требования *подотчетности*).

Семейства в пределах класса различаются по строгости и другим нюансам требований.

Компонент - минимальный набор требований, фигурирующий как целое.

Элемент - неделимое требование.

Основные понятия

Как и между библиотечными функциями, между компонентами ОК могут существовать зависимости. Они возникают, когда компонент сам по себе недостаточен для достижения **цели безопасности**. Вообще говоря, не все комбинации компонентов имеют смысл, и понятие зависимости в какой-то степени компенсирует недостаточную выразительность библиотечной организации, хотя и не заменяет объединение функций в содержательные объектные интерфейсы.

Основные понятия

Как указывалось выше, с помощью библиотек могут формироваться два вида нормативных документов: профиль защиты и задание по безопасности.

Профиль защиты (ПЗ) представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

Основные понятия

Выше мы отмечали, что в ОК нет готовых классов защиты. Сформировать классификацию в терминах "Общих критериев" - значит определить несколько иерархически упорядоченных (содержащих усиливающиеся требования) профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования **доверия безопасности**.

Основные понятия

Выделение некоторого подмножества из всего множества профилей защиты во многом носит субъективный характер. По целому ряду соображений (одним из которых является желание придерживаться объектно-ориентированного подхода) целесообразно, на наш взгляд, сформировать сначала отправную точку классификации, выделив базовый (минимальный) ПЗ, а дополнительные требования компоновать в функциональные пакеты.

Основные понятия

Функциональный пакет - это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности. "Общие критерии" не регламентируют структуру пакетов, процедуры *верификации*, регистрации и т.п., отводя им роль технологического средства формирования ПЗ.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

Функциональные требования

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в "Общих критериях" представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это, конечно, значительно больше, чем число аналогичных сущностей в "Оранжевой книге".

Перечислим классы функциональных требований ОК:

- *идентификация* и *аутентификация*;
- **защита данных пользователя**;
- **защита функций безопасности** (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);

Функциональные требования

- **управление безопасностью** (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
- **аудит безопасности** (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
- **доступ к объекту оценки**;
- **приватность** (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
- **использование ресурсов** (требования к доступности информации);

Функциональные требования

- **криптографическая поддержка** (управление ключами);
- **связь** (*аутентификация* сторон, участвующих в обмене данными);
- **доверенный маршрут/канал** (для связи с сервисами безопасности).

Опишем подробнее два класса, демонстрирующие особенности современного подхода к ИБ.

Класс "Приватность" содержит 4 семейства функциональных требований.

Функциональные требования

Анонимность. Позволяет выполнять действия без раскрытия идентификатора пользователя другим пользователям, субъектам и/или объектам. Анонимность может быть полной или выборочной. В последнем случае она может относиться не ко всем операциям и/или не ко всем пользователям (например, у уполномоченного пользователя может оставаться возможность выяснения идентификаторов пользователей).

Псевдонимность. Напоминает анонимность, но при применении псевдонима поддерживается ссылка на идентификатор пользователя для обеспечения *подотчетности* или для других целей.

Функциональные требования

Невозможность ассоциации. Семейство обеспечивает возможность неоднократного использования информационных сервисов, но не позволяет ассоциировать случаи использования между собой и приписать их одному лицу. Невозможность ассоциации защищает от построения профилей поведения пользователей (и, следовательно, от получения информации на основе подобных профилей).

Функциональные требования

Скрытность. Требования данного семейства направлены на то, чтобы можно было использовать информационный сервис с сокрытием факта использования. Для *реализации* скрытности может применяться, например, широковещательное распространение информации, без указания конкретного адресата. Годятся для *реализации* скрытности и методы стеганографии, когда скрывается не только содержание сообщения (как в криптографии), но и сам факт его отправки.

Еще один показательный (с нашей точки зрения) класс функциональных требований - "Использование ресурсов", содержащий требования доступности. Он включает три семейства.

Функциональные требования

Отказоустойчивость. Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В ОК различаются активная и пассивная отказоустойчивость. Активный механизм содержит специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.

Функциональные требования

Обслуживание по приоритетам. Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.
Распределение ресурсов. Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.

Мы видим, что "Общие критерии" - очень продуманный и полный документ с точки зрения функциональных требований. В то же время, хотелось бы обратить внимание и на некоторые недостатки.

Функциональные требования

Первый мы уже отмечали - это отсутствие объектного подхода. Функциональные требования не сгруппированы в осмысленные наборы (объектные интерфейсы), к которым могло бы применяться наследование. Подобное положение, как известно из технологии программирования, чревато появлением слишком большого числа комбинаций функциональных компонентов, несопоставимых между собой.

В современном программировании ключевым является вопрос накопления и многократного использования знаний. Стандарты - одна из форм накопления знаний. Следование в ОК "библиотечному", а не объектному подходу сужает круг фиксируемых знаний, усложняет их корректное использование.

Функциональные требования

К сожалению, в "Общих критериях" отсутствуют архитектурные требования, что является естественным следствием избранного старомодного программистского подхода "снизу вверх". На наш взгляд, это серьезное упущение. Технологичность средств безопасности, следование общепризнанным рекомендациям по протоколам и программным интерфейсам, а также апробированным архитектурным решениям, таким как менеджер/агент, - необходимые качества изделий информационных технологий, предназначенных для поддержки критически важных функций, к числу которых, безусловно, относятся функции безопасности.

Функциональные требования

Без рассмотрения интерфейсных аспектов системы оказываются нерасширяемыми и изолированными. Очевидно, с практической точки зрения это недопустимо. В то же время, обеспечение безопасности интерфейсов - важная задача, которую желательно решать единообразно.

Требования доверия безопасности

Установление доверия безопасности, согласно "Общим критериям", основывается на активном исследовании объекта оценки.

Форма представления требований доверия, в принципе, та же, что и для функциональных требований. Специфика состоит в том, что каждый элемент требований доверия принадлежит одному из трех типов:

- действия **разработчиков**;
- представление и содержание **свидетельств**;
- действия **оценщиков**.

Требования доверия безопасности

- Всего в ОК 10 классов, 44 семейства, 93 компонента требований доверия безопасности. Перечислим классы:

- разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до *реализации*);
- поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);
- *тестирование*;
- **оценка уязвимостей** (включая оценку стойкости функций безопасности);
- **поставка и эксплуатация**;

Требования доверия безопасности

- управление конфигурацией;
- руководства (требования к эксплуатационной документации);
- **поддержка доверия** (для поддержки этапов жизненного цикла после сертификации);
- оценка профиля защиты;
- оценка задания по безопасности.

Применительно к требованиям доверия в "Общих критериях" сделана весьма полезная вещь, не реализованная, к сожалению, для функциональных требований. А именно, введены так называемые оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.

Требования доверия безопасности

Оценочный уровень доверия 1 (начальный) предусматривает анализ **функциональной спецификации**, спецификации интерфейсов, эксплуатационной документации, а также независимое *тестирование*. Уровень применим, когда угрозы не рассматриваются как серьезные.

Оценочный уровень доверия 2, в дополнение к первому уровню, предусматривает наличие **проекта верхнего уровня** объекта оценки, выборочное независимое *тестирование*, анализ стойкости функций безопасности, поиск разработчиком явных уязвимых мест.

Требования доверия безопасности

На третьем уровне ведется контроль среды разработки и управление конфигурацией объекта оценки.

На уровне 4 добавляются полная спецификация интерфейсов, **проекты нижнего уровня**, анализ подмножества *реализации*, применение неформальной **модели** *политики безопасности*, независимый анализ уязвимых мест, автоматизация управления конфигурацией. Вероятно, это самый высокий уровень, которого можно достичь при существующей технологии программирования и приемлемых затратах.

Требования доверия безопасности

Уровень 5, в дополнение к предыдущим, предусматривает применение формальной модели *политики безопасности*, полуформальных функциональной спецификации и проекта верхнего уровня с **демонстрацией соответствия** между ними. Необходимо проведение анализа скрытых каналов разработчиками и оценщиками.

На уровне 6 *реализация* должна быть представлена в структурированном виде. Анализ соответствия распространяется на проект нижнего уровня.

Требования доверия безопасности

Оценочный уровень 7 (самый высокий) предусматривает формальную *верификацию* проекта объекта оценки. Он применим к ситуациям чрезвычайно высокого риска.

На этом мы заканчиваем краткий обзор "Общих критериев".

Гармонизированные критерии Европейских стран

Наше изложение "Гармонизированных критериев" основывается на версии 1.2, опубликованной в июне 1991 года от имени соответствующих органов четырех стран - Франции, Германии, Нидерландов и Великобритании. Принципиально важной чертой Европейских Критериев является отсутствие требований к условиям, в которых должна работать информационная система. Так называемый **спонсор**, то есть организация, запрашивающая сертификационные услуги, формулирует цель оценки, то есть описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции.

Гармонизированные критерии Европейских стран

Задача органа сертификации - оценить, насколько полно достигаются поставленные цели, то есть насколько корректны и эффективны архитектура и *реализация* **механизмов безопасности** в описанных спонсором условиях. Таким образом, в терминологии "Оранжевой книги", Европейские Критерии относятся к гарантированности безопасной работы системы. Требования к *политике безопасности* и наличию защитных механизмов не являются составной частью Критериев. Впрочем, чтобы облегчить формулировку цели оценки, Критерии содержат в качестве приложения описание десяти классов функциональности, типичных для правительственных и коммерческих систем.

Гармонизированные критерии Европейских стран

Европейские Критерии рассматривают все основные составляющие информационной безопасности - **конфиденциальность**, **целостность**, **доступность**. В 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.

Гармонизированные критерии Европейских стран

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.

Из практических соображений важно обеспечить единство критериев оценки продуктов и систем - например, чтобы облегчить оценку системы, составленной из ранее сертифицированных продуктов. По этой причине для систем и продуктов вводится единый термин - объект оценки.

Гармонизированные критерии Европейских стран

Каждая система и/или продукт предъявляет свои требования к обеспечению конфиденциальности, целостности и доступности. Чтобы удовлетворить эти требования, необходимо предоставить соответствующий набор **функций (сервисов) безопасности**, таких как *идентификация* и *аутентификация*, управление доступом или *восстановление после сбоев*.

Гармонизированные критерии Европейских стран

Сервисы безопасности реализуются посредством конкретных механизмов. Чтобы объекту оценки можно было доверять, необходима определенная степень уверенности в наборе функций и механизмов безопасности. Степень уверенности мы будем называть гарантированностью. Гарантированность может быть большей или меньшей в зависимости от тщательности проведения оценки.

Гармонизированные критерии Европейских стран

Гарантированность затрагивает два аспекта - **эффективность** и **корректность** средств безопасности. При проверке эффективности анализируется соответствие между целями, сформулированными для объекта оценки, и имеющимся набором функций безопасности. Точнее говоря, рассматриваются вопросы адекватности функциональности, взаимной согласованности функций, простоты их использования, а также возможные последствия эксплуатации известных 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.

Гармонизированные критерии Европейских стран

Под корректностью понимается правильность *реализации* функций и механизмов безопасности. В Критериях определяется семь возможных *уровней гарантированности* корректности - от E0 до E6 (в порядке возрастания). Уровень E0 означает отсутствие гарантированности. При проверке корректности анализируется весь жизненный цикл объекта оценки - от *проектирования* до эксплуатации и *сопровождения*. градации мощности - базовая, средняя и высокая.

Гармонизированные критерии Европейских стран

Общая оценка системы складывается из минимальной мощности механизмов безопасности и *уровня гарантированности* корректности.

Гармонизированные критерии Европейских стран явились для своего времени весьма передовым стандартом, они создали предпосылки для появления "Общих критериев".

Интерпретация "Оранжевой книги" для сетевых конфигураций

В 1987 году Национальным центром компьютерной безопасности США была опубликована интерпретация "Оранжевой книги" для сетевых конфигураций. Данный документ состоит из двух частей. Первая содержит собственно интерпретацию, во второй рассматриваются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

Интерпретация "Оранжевой книги" для сетевых конфигураций

В первой части вводится минимум новых понятий. Важнейшее из них - **сетевая доверенная вычислительная база**, распределенный аналог *доверенной вычислительной базы* изолированных систем. Сетевая доверенная вычислительная база формируется из всех частей всех компонентов сети, обеспечивающих информационную безопасность. Доверенная сетевая система должна обеспечивать такое распределение защитных механизмов, чтобы общая *политика безопасности* реализовывалась, несмотря на уязвимость коммуникационных путей и на параллельную, асинхронную работу компонентов.

Интерпретация "Оранжевой книги" для сетевых конфигураций

Прямой зависимости между вычислительными базами компонентов, рассматриваемых как изолированные системы, и фрагментами сетевой вычислительной базы не существует. Более того, нет прямой зависимости и между уровнями безопасности отдельных компонентов и уровнем безопасности всей сетевой конфигурации. Например, в результате объединения двух систем класса B1, обладающих несовместимыми правилами кодирования *меток безопасности*, получается сеть, не удовлетворяющая требованию целостности меток.

Интерпретация "Оранжевой книги" для сетевых конфигураций

В качестве противоположного примера рассмотрим объединение двух компонентов, один из которых сам не обеспечивает протоколирование действий пользователя, но передает необходимую информацию другому компоненту, который и ведет протокол. В таком случае распределенная система в целом, несмотря на слабость компонента, удовлетворяет требованию *подотчетности*.

Интерпретация "Оранжевой книги" для сетевых конфигураций

Чтобы понять суть положений, вошедших в первую часть, рассмотрим интерпретацию требований к *классу безопасности* C2. Первое требование к этому классу - поддержка *произвольного управления доступом*. Интерпретация предусматривает различные варианты распределения сетевой доверенной вычислительной базы по компонентам и, соответственно, различные варианты распределения механизмов управления доступом. В частности, некоторые компоненты, закрытые для прямого доступа пользователей, могут вообще не содержать подобных механизмов.

Интерпретация "Оранжевой книги" для сетевых конфигураций

Интерпретация отличается от самих "Критериев" учетом динамичности сетевых конфигураций. Предусматривается наличие средств проверки подлинности и корректности функционирования компонентов перед их включением в сеть, наличие протокола взаимной проверки компонентами корректности функционирования друг друга, а также присутствие средств оповещения администратора о неполадках в сети. Сетевая конфигурация должна быть устойчива к отказам отдельных компонентов или коммуникационных путей.

Интерпретация "Оранжевой книги" для сетевых конфигураций

Среди защитных механизмов в сетевых конфигурациях на первом месте стоит **криптография**, помогающая поддерживать как конфиденциальность, так и целостность. Следствием использования криптографических методов является необходимость *реализации* механизмов управления ключами.

Интерпретация "Оранжевой книги" для сетевых конфигураций

Систематическое рассмотрение вопросов доступности является новшеством по сравнению не только с "Оранжевой книгой", но и с рекомендациями X.800. Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в обслуживании пользователей. *Доверенная система* должна иметь возможность обнаруживать ситуации недоступности, уметь возвращаться к нормальной работе и противостоять атакам на доступность.

Интерпретация "Оранжевой книги" для сетевых конфигураций

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

- внесение в конфигурацию той или иной формы **избыточности** (резервное оборудование, запасные каналы связи и т.п.);
- наличие средств **реконфигурирования** для изоляции и/или замены узлов или коммуникационных каналов, отказавших или подвергшихся атаке на доступность;
- **рассредоточенность** сетевого **управления**, отсутствие **единой точки отказа**;

Интерпретация "Оранжевой книги" для сетевых конфигураций

- наличие средств **нейтрализации отказов** (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов);
- выделение **подсетей** и **изоляция** групп **пользователей** друг от друга.

Одним из важнейших в "Оранжевой книге" является понятие *монитора обращений*. Применительно к структурированию сетевой конфигурации можно сформулировать следующее утверждение, обеспечивающее достаточное условие корректности фрагментирования *монитора обращений*.

Интерпретация "Оранжевой книги" для сетевых конфигураций

Пусть каждый субъект (то есть процесс, действующий от имени какого-либо пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Далее, пусть каждый компонент содержит свой *монитор обращений*, отслеживающий все локальные попытки доступа, и все мониторы реализуют согласованную *политику безопасности*. Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый *монитор обращений* для всей сетевой конфигурации.

Интерпретация "Оранжевой книги" для сетевых конфигураций

Данное утверждение является теоретической основой декомпозиции распределенной ИС в объектно-ориентированном стиле в сочетании с криптографической защитой коммуникаций.

Руководящие документы Гостехкомиссии России

Гостехкомиссия России ведет весьма активную нормотворческую деятельность, выпуская Руководящие документы (РД), играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления Гостехкомиссия России выбрала ориентацию на "Общие критерии", что можно только приветствовать.

Руководящие документы Гостехкомиссии России

В своем обзоре мы рассмотрим два важных, хотя и не новых, Руководящих документа - Классификацию **автоматизированных систем (АС)** по уровню **защищенности от несанкционированного доступа (НСД)** и аналогичную Классификацию **межсетевых экранов (МЭ)**.

Согласно первому из них, устанавливается девять классов защищенности АС от НСД к информации.

Руководящие документы Гостехкомиссии России

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Руководящие документы Гостехкомиссии России

Третья группа классифицирует АС, в которых работает один пользователь, имеющий доступ ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранящейся на носителях различного уровня конфиденциальности.

Группа содержит два класса - 2Б и 2А.

Руководящие документы Гостехкомиссии России

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

Сведем в таблицу требования ко всем девяти классам защищенности АС.

Руководящие документы Гостехкомиссии России

Таблица 5.3. Требования к защищенности автоматизированных систем

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом 1.1. *Идентификация*, проверка подлинности и контроль доступа субъектов: в систему;	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	-	-	-	+	-	+	+	+	+
к программам;	-	-	-	+	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей.	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации	-	-	-	+	-	-	+	+	+
2. Подсистема регистрации и учета 2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети);	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов;	-	+	-	+	-	+	+	+	+
запуска/завершения программ и процессов (заданий, задач);	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	-	-	-	+	-	+	+	+	+
изменения полномочий субъектов доступа;	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа.	-	-	-	+	-	-	+	+	+

Руководящие документы Гостехкомиссии России

2.2. Учет носителей информации.	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.	-	+	-	+	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты.	-	-	-	-	-	-	+	+	+
3. Криптографическая подсистема 3.1. Шифрование конфиденциальной информации.	-	-	-	+	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах.	-	-	-	-	-	-	-	-	+
3.3. Использование аттестованных (сертифицированных) криптографических средств.	-	-	-	+	-	-	-	+	+
4. Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации.	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации.	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы защиты) информации в АС.	-	-	-	+	-	-	+	+	+
4.4. Периодическое *тестирование* СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты.	-	+	-	+	-	-	+	+	+

"-" нет требований к данному классу;

"+" есть требования к данному классу;

"СЗИ НСД" система защиты информации от несанкционированного доступа

Руководящие документы Гостехкомиссии России

По существу перед нами - минимум требований, которым необходимо следовать, чтобы обеспечить конфиденциальность информации. Целостность представлена отдельной подсистемой (номер 4), но непосредственно к интересующему нас предмету имеет отношение только пункт 4.1. Доступность (точнее, восстановление) предусмотрено только для самих средств защиты.

Руководящие документы Гостехкомиссии России

Переходя к рассмотрению второго РД Гостехкомиссии России - Классификации межсетевых экранов - укажем, что данный РД представляется нам принципиально важным, поскольку в нем идет речь не о целостном продукте или системе, а об отдельном сервисе безопасности, обеспечивающем межсетевое разграничение доступа.

Данный РД важен не столько содержанием, сколько самим фактом своего существования.

Руководящие документы Гостехкомиссии России

Основным критерием классификации МЭ служит протокольный уровень (в соответствии с эталонной семиуровневой моделью), на котором осуществляется **фильтрация информации**. Это понятно: чем выше уровень, тем больше информации на нем доступно и, следовательно, тем более тонкую и надежную фильтрацию можно реализовать.

Значительное внимание в РД уделено собственной безопасности служб обеспечения защиты и вопросам согласованного администрирования распределенных конфигураций.