**Руководящие документы Гостехкомиссии России**

Гостехкомиссия России в период своего существования вела 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.

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.

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*.

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.

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*.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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. | - | - | - | + | - | - | + | + | + |
| 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

*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.

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.

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.