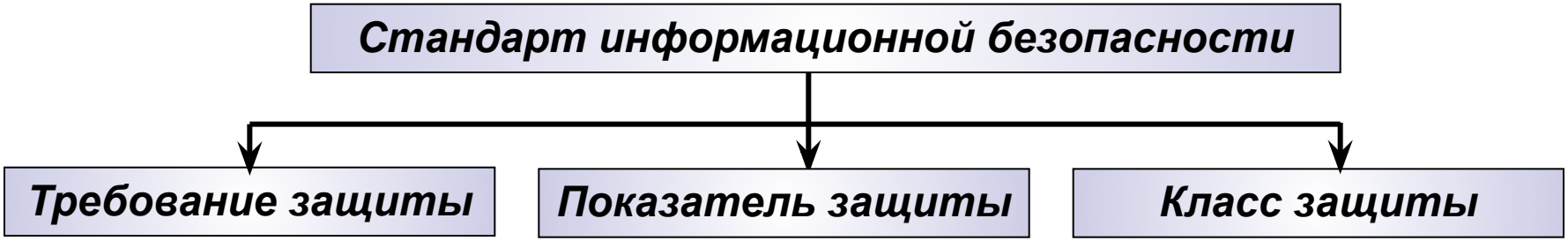
Лекция – Стандарты в области информационной безопасности в РФ

1 Введение

Стандарт информационной безопасности – ***нормативный документ, определяющий порядок и правила взаимодействия субъектов информационных отношений, а также требования к инфраструктуре информационной системы, обеспечивающие необходимый уровень информационной безопасности.***



Федеральная служба по техническому и экспортному контролю Российской Федерации (ФСТЭК России) — *федеральный орган исполнительной власти России, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности.*

2 ФСТЭК и его роль в обеспечении информационной безопасности в РФ

В Российской Федерации информационная безопасность обеспечивается соблюдение указов Президента, федеральных законов, постановлений Правительства Российской Федерации, руководящих документов ФСТЭК России и других нормативных документов.

Наиболее общие документы были рассмотрены ранее при изучении правовых основ информационной безопасности. В РФ с точки зрения стандартизации положений в сфере информационной безопасности первостепенное значение имеют руководящие документы (РД) ***ФСТЭК России***, одной из задач которой является "проведение единой государственной политики в области технической защиты информации".

ФСТЭК России ведет весьма активную нормотворческую деятельность, выпуская руководящие документы, играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления ФСТЭК России выбрала ориентацию на "Общие критерии".

За 10 лет своего существования ***ФСТЭК разработала*** и довела до уровня национальных стандартов ***десятки документов***, среди которых:

- ***Руководящий документ "Положение по аттестации объектов информатизации по требованиям безопасности информации"*** (Утверждено Председателем ФСТЭК России 25.11.1994 г.).

- ***Руководящий документ "Автоматизированные системы (АС). Защита от несанкционированного доступа (НСД) к информации. Классификация АС и требования к защите информации"*** (ФСТЭК России, 1997 г.).

- ***Руководящий документ "Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации"*** (ФСТЭК России, 1992 г.).

- ***Руководящий документ "Концепция защиты средств вычислительной техники от НСД к информации"*** (ФСТЭК России, 1992 г.).

- ***Руководящий документ "Защита от НСД к информации. Термины и определения"*** (ФСТЭК России, 1992 г.).
- ***Руководящий документ "Средства вычислительной техники (СВТ). Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации"*** (ФСТЭК России, 1997 г.).
- ***Руководящий документ "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей"*** (ФСТЭК России, 1999 г.).
- ***Руководящий документ "Специальные требования и рекомендации по технической защите конфиденциальной информации"*** (ФСТЭК России, 2001 г.).

3 Документы по оценке защищенности автоматизированных систем в РФ

Руководящий документ ***"СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"*** устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Основой для разработки этого документа явилась "Оранжевая книга". Этот оценочный стандарт устанавливается ***семь классов защищенности*** СВТ от НСД к информации.

Самый низкий класс – седьмой, самый высокий – первый. ***Классы*** подразделяются на ***четыре группы***, отличающиеся уровнем защиты:

I. первая группа содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов;
II. вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
III. третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
IV. четвертая группа характеризуется верифицированной защитой и включает только первый класс.

Руководящий документ ***"АС. Защита от НСД к информации. Классификация АС и требования по защите информации"*** устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

К числу определяющих признаков, по которым производится группировка АС в ***различные классы***, относятся:

I. наличие в АС информации различного уровня конфиденциальности;
II. уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
III. режим обработки данных в АС – коллективный или индивидуальный.

В документе определены ***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 и конфиденциальности информации и, следовательно, иерархия классов защищенности АС.

Таблица 2 - 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.									

Руководящий документ ***"СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации"*** является основным документом для анализа системы защиты внешнего периметра корпоративной сети. Данный документ определяет показатели защищенности межсетевых экранов (МЭ). Каждый показатель защищенности представляет собой набор требований безопасности, характеризующих определенную область функционирования МЭ.

Всего выделяется ***пять показателей защищенности***:

- ✔управление доступом;
- ✔идентификация и аутентификация;
- ✔регистрация событий и оповещение;
- ✔контроль целостности;
- ✔восстановление работоспособности.

На основании показателей защищенности определяются следующие ***пять классов защищенности МЭ***:

- ✔простейшие фильтрующие маршрутизаторы – 5 класс;
- ✔пакетные фильтры сетевого уровня – 4 класс;
- ✔простейшие МЭ прикладного уровня – 3 класс;
- ✔мЭ базового уровня – 2 класс;
- ✔продвинутые МЭ – 1 класс.

МЭ первого класса защищенности могут использоваться в АС класса 1А, обрабатывающих информацию "Особой важности". ***Второму классу защищенности МЭ*** соответствует класс защищенности АС 1Б, предназначенный для обработки "совершенно секретной" информации и т. п.

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.