



Курс: **основы информационной безопасности**

Тема: **Законодательство в области ИБ АС**

Преподаватель: Пятков
Антон Геннадьевич

Красноярск

Законодательная система РФ

**Конституция и
конституционные
акты
(Кодексы, ФЗ, указы)**

Акты правительства
(постановления
правительства)

Положения и стандарты, приказы,
инструкции и другие нормативно-
правовые акты, разработанные и
утвержденные на уровне министерств,
регуляторов;

Положения и стандарты, инструкции и другие
нормативно-правовые акты, разработанные и
утвержденные на уровне предприятий, организаций,
зарегистрированные акты физических лиц.

НПА
предприятия

Конституция

К построению системы ИБ относятся все статьи Конституции (1993 г.), касающиеся информации и информационного обмена (ст. 23, ст. 24, ст. 29).

Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.
2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение допускается только на основании судебного решения (СОПМ).

Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.
2. Органы гос. власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 29

1. Каждому гарантируется свобода мысли и слова.
2. Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства.
3. Никто не может быть принужден к выражению своих мнений и убеждений или отказу от них
4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих ГТ, определяется ФЗ.
5. Гарантируется свобода массовой информации. Цензура запрещается.

Законы

Гражданский кодекс (договоры, частные дела, гражданские права)

Трудовой кодекс (трудовые права и свободы граждан)

Уголовный кодекс ст. 183 ч. 1 (Незаконные получ./разглаш. КТ, налоговой, банковской)

Против конституционных прав и свобод ст. 136, 137, 138, 140, 143, 146, 148

Преступления в сфере компьютерной безопасности ст. 272; 273; 274

Налоговый кодекс ст. 102 (Налоговая тайна)

Основы законодательства РФ об Архивном фонде РФ архивах

ФЗ «Об информации, информатизации и защите информации», «О государственной тайне», «О коммерческой тайне», «О персональных данных», «О цифровой подписи», «О безопасности», «О техническом регулировании», «Об обеспечении единства измерений», «О лицензировании отдельных видов деятельности», «О связи», «О федеральных органах правительственной связи и информации», «Об участии в международном информационном обмене», «Об авторском праве и смежных правах»...

Доктрина ИБ РФ, Политика Информационной Безопасности (ПиБ) РФ,
Концепция Национальной Безопасности РФ

Доктрина ИБ РФ № Пр-1895



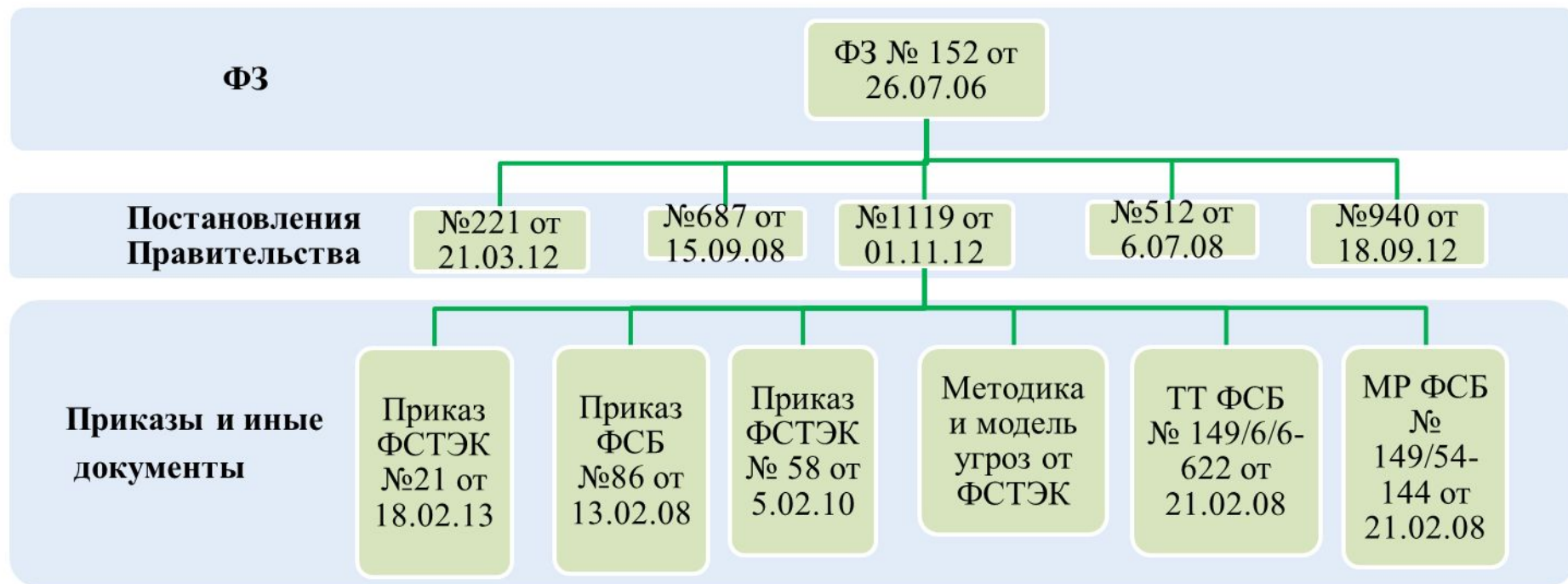
Национальные интересы РФ в информационной сфере и их обеспечение:

- ✓ соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;
- ✓ информационное обеспечение государственной политики РФ (информирование о политике РФ, доступ к открытым ГИС, ресурсам);
- ✓ развитие современных информационных технологий, отечественной индустрии информации, обеспечение потребностей внутреннего рынка её продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- ✓ защита информационных ресурсов от НСД, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории РФ.



Пример иерархии документов

Иерархия документов по защите ПДн согласно законодательства РФ



НПА по ЗИ

Стандарты:

- ✓ Руководящий документ (РД ГТК) «Концепция защиты СВТ и АС от НСД к информации» (практические рекомендации по ЗИ, содержащей ГТ);
- ✓ Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К);
- ✓ ГОСТ Р 51583-2000 «Порядок создания АС в защищенном исполнении»;
- ✓ ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ»;
- ✓ ...

Приказы ФСТЭК, ФСБ, Мининформсвязи России

- ✓ Приказ ФСБ № 378 от 10.07.2014 (Описаны орг. и технические меры по обеспечению ИБ ПДн при их обработке в ИСПДн с использованием СКЗИ);
- ✓ Приказ ФСТЭК № 17 от 11.02.2013 (Описаны требования ЗИ, не составляющей ГТ, содержащейся в государственных информационных системах);
- ✓ Приказ ФСТЭК № 21 от 18.02.2013 (Описаны организационные и технические меры по обеспечению ИБ ПДн в ИСПДн);
- ✓ Приказ ФСТЭК № 31 от 14.03.2014 (Описаны требования ЗИ в АС управления производственными и технологическими процессами);
- ✓ ...

Рекомендуемые к использованию документы международных стандартов (ISO 7799 Управление ИБ, ISO/IEC TR 13335 ИТ. Руководство по управлению ИБ...)»

Классы защищённости АС от НСД

Документы ГТК устанавливают 9 классов защищенности АС от НСД, распределенных по 3 группам. Каждый класс характеризуется определенной совокупностью требований к средствам защиты.

Обозначение: класс защищённости=группа+категория информации.

Группа 1: многопользовательские АС, одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять 5 - 1Д, 1Г, 1В, 1Б и 1А.

Группа 2: все пользователи имеют одинаковые права доступа ко всей информации АС. Группа содержит 2 класса - 2Б и 2А.

Группа 3: работает один пользователь с информацией одного уровня конфиденциальности. Группа содержит 2 класса - 3Б и 3А.

Категории информации:

А – ОВ (особой важности)

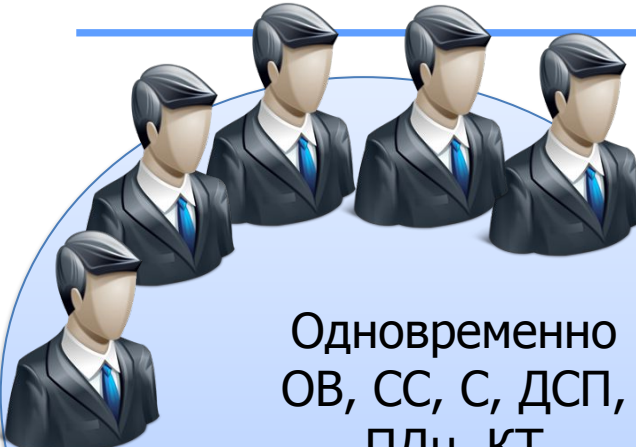
Б – СС (совершенно секретно)

В – С (секретно) + "ПДн"

Г – ДСП (для служебного просмотра) + "ПДн"

Д – КТ (Коммерческая тайна)

Классы защищённости АС от НСД



Одновременно
ОВ, СС, С, ДСП,
ПДн, КТ

1Д, 1Г, 1В, 1Б, 1А



только ОВ
или
только СС

2Б и 2А



только ОВ
или
только СС

3Б и 3А

РД. АС. Защита от НСД к информации

Подсистемы и требования	Классы				
	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 уст-вам	-	+	+	+	+
к программам	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей	-	+	+	+	+
1.2. Управление потоками информации	-	-	+	+	+
2. Подсистема регистрации и учета					
2.1. Регистрация и учёт:					
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+	+	+	+
выдачи печатных (графических) выходных документов	-	+	+	+	+
запуска (завершения) программ и процессов (заданий, задач)	-	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам	-	+	+	+	+
доступа программ к терминалам, ЭВМ, узлам сети, внешним устройствам,	-	+	+	+	+
томам, файлам, полям записей и пр.					
изменения полномочий субъектов доступа	-	-	+	+	+
создаваемых защищаемых объектов доступа	-	-	+	+	+
2.2. Учет носителей информации	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной					
памяти ЭВМ, устройств и носителей	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты	-	-	+	+	10

РД. АС. Защита от НСД к информации

Подсистемы и требования	Классы				
	1Д	1Г	1В	1Б	1А
3. Криптографическая подсистема					
3.1. Шифрование конфиденциальной информации	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам доступа) на разных ключах	-	-	-	-	+
3.3. Использование аттестованных (сертифицированных) СКЗИ	-	-	-	+	+
4. Подсистема обеспечения целостности					
4.1. Обеспечение целостности программных средств и обрабатываемой инф-ии	+	+	+	+	+
4.2. Физич.охрана свт 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	-	-	+	+	+