

Начала информационной безопасности

Попов Николай Александрович

*кандидат экономических наук, доцент по кафедре
безопасности информационных технологий.*

Тел. моб. 8-983-163-9493 E-mail: naporov2005@yandex.ru

Выписка из федерального закона Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и защите информации

- **Статья 16. Защита информации**
- 1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:
 - 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
 - 2) соблюдение конфиденциальности информации ограниченного доступа,
 - 3) реализацию права на доступ к информации.

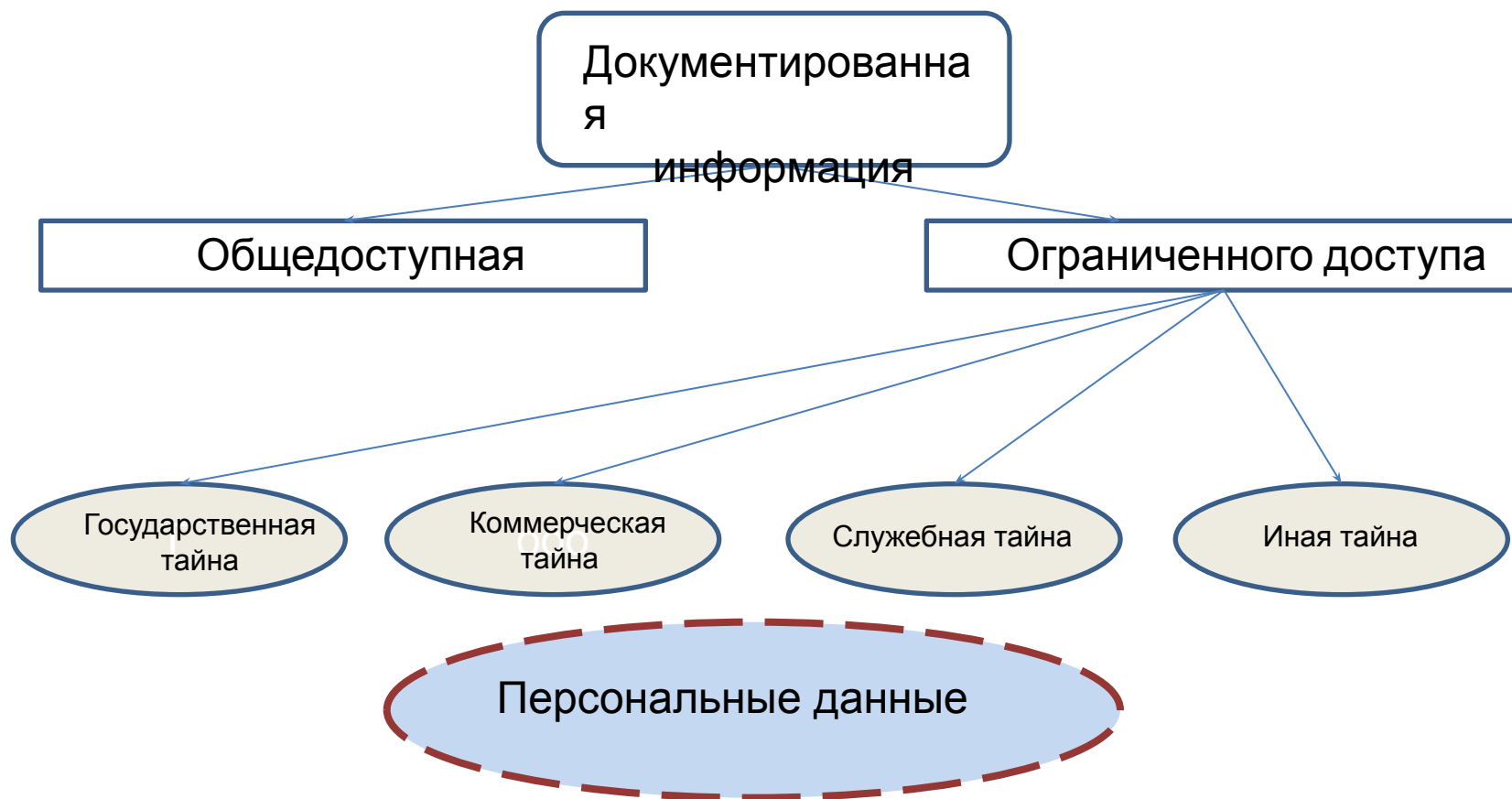
Выписка из федерального закона Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и защите информации

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

- 1) информация - сведения (сообщения, данные) независимо от формы их представления;
- 5) обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- 7) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- 11) документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
- 12) оператор информационной системы - гражданин или юридическое

Классификация документированной информации

(в соответствии с федеральным законом Российской Федерации от 27 июля 2006 г. N 149-ФЗ)



Профессиональная тайна

Банковская тайна

Нотариальная тайна

Процессуальные тайны

Врачебная тайна

Адвокатская тайна

Тайна страхования

Тайна связи

Тайна усыновления

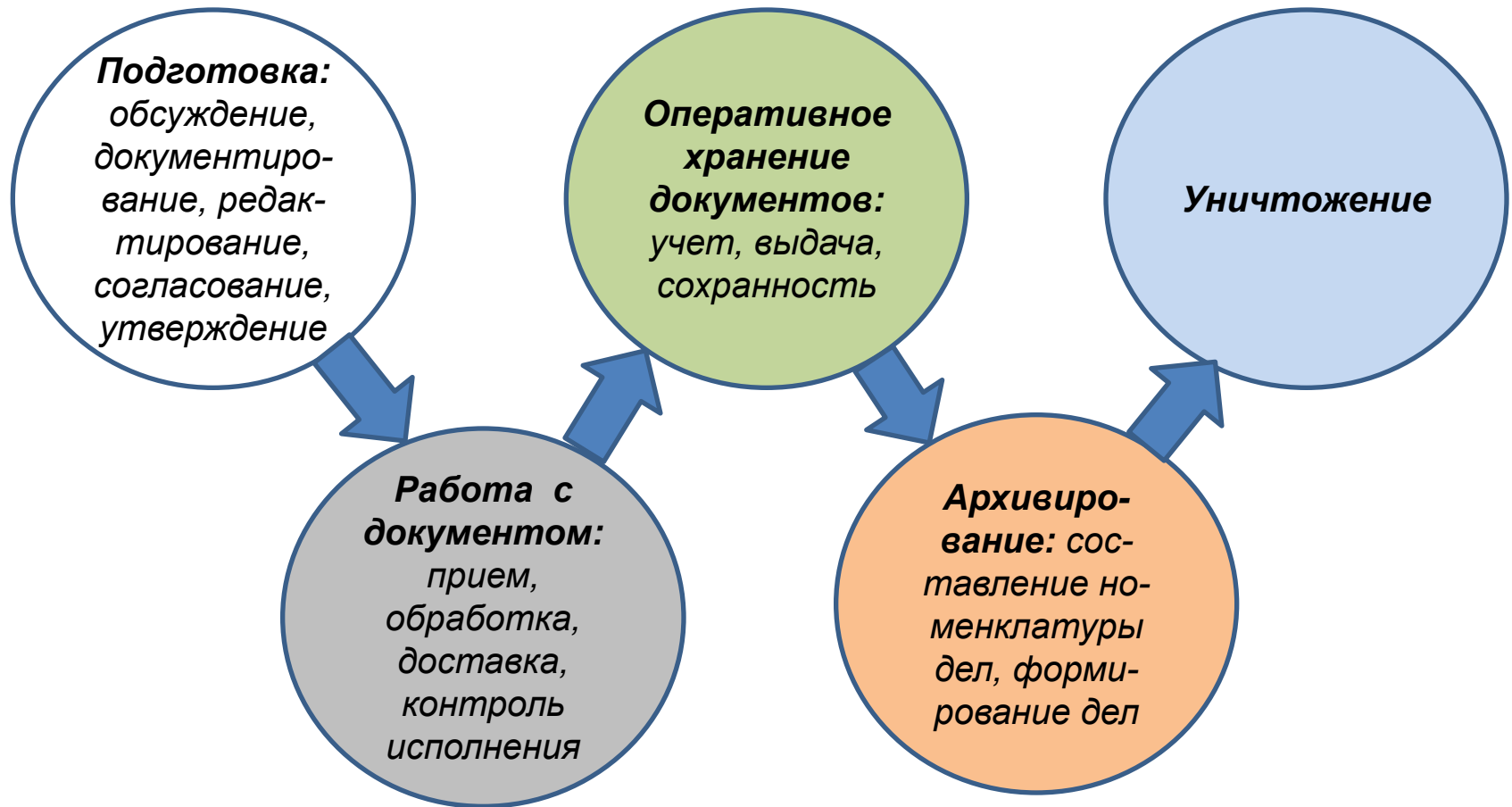
Тайна исповеди

Укрупненный план организационных мероприятий, направленных на обеспечение информационной безопасности

(Что? Кто? Где? Каким образом?)

- Установление перечня сведений, которые следует отнести к категории «тайна».
- Определение круга лиц, допускаемых к работе с информацией ограниченного доступа.
- Нормативное закрепление помещений, в которых разрешена работа с информацией ограниченного доступа.
- Закрепление технических средств за системой, в которой ведется обработка информации ограниченного доступа.

Технологические этапы в документообороте



Каналы утечки информации, возникающие в процессе подготовки документа

- ***Акустические (вибраакустические):***
 - открытые окна, форточки;
 - вентиляция;
 - двери;
 - стены и перекрытия и др.
- ***Оптические:***
 - через окна;
 - визуально (на месте подготовки документа) и др.
- ***Радиоэлектронные (акустоэлектрические):***
 - приемопередающие устройства;
 - телефонные аппараты;
 - провода, выходящие за пределы контролируемой зоны и др.

Каналы утечки информации, возникающие в дальнейшей работе с документом

- несанкционированный доступ к информации;

- паразитные сигналы и наводки;

- цепи электропитания;

- цепи заземления и др.

Требования к безопасности информационных систем в России

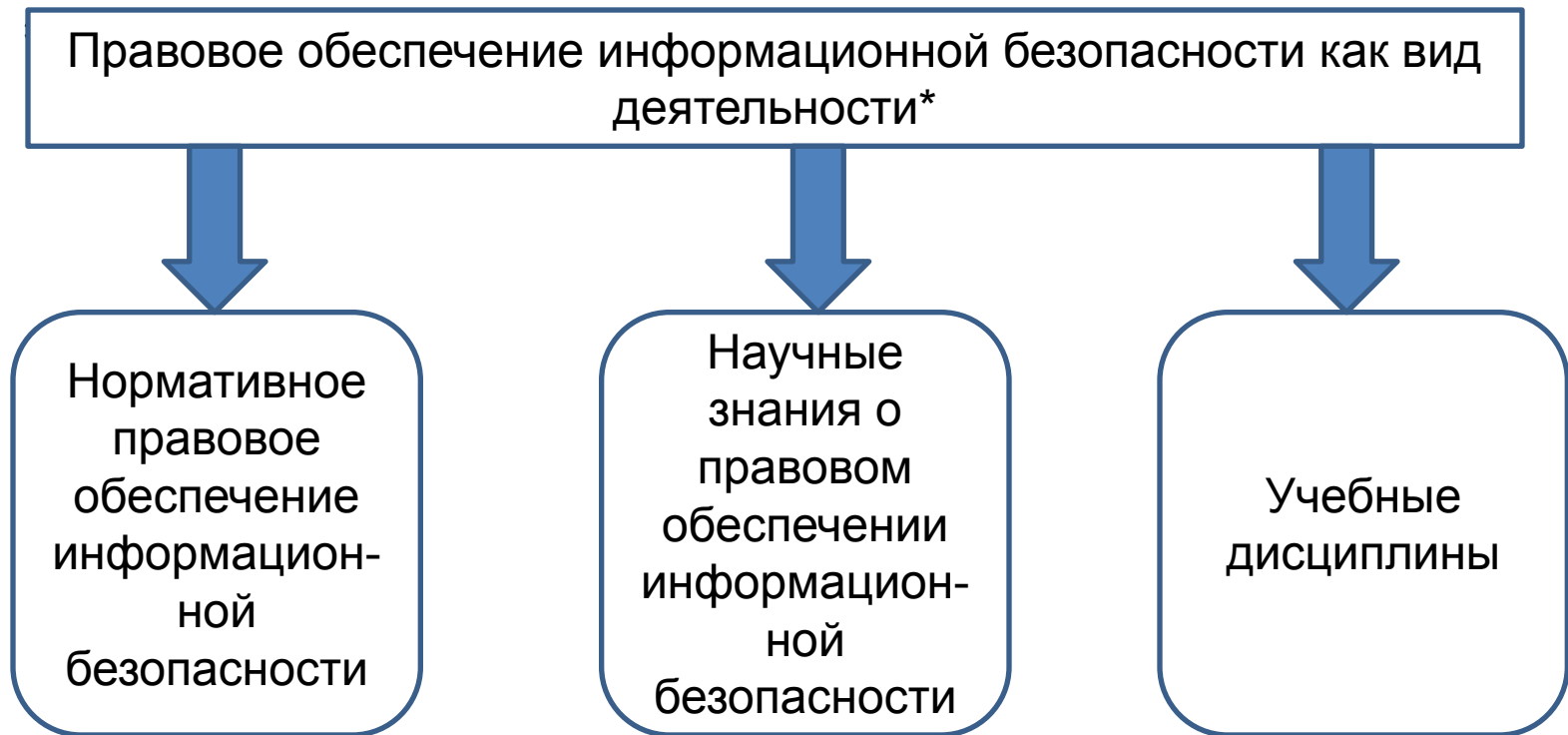
сформулированы в руководящем документе Государственной технической комиссией при Президенте РФ «Классификация автоматизированных систем и требований по защите информации» выпущенном в 1992 году, в котором выделено 9 классов защищенности автоматизированных систем от несанкционированного доступа к информации.

По специфике обработки информации классы разделены на группы:

- третья группа – системы в которых работает один пользователь, допущенный ко всей обрабатываемой информации (классы 3Б и 3А);
- вторая группа – системы в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации (классы 2Б и 2А);
- первая группа – многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, причем различные пользователи имеют разные права на доступ к информации (классы 1Д, 1Г, 1В, 1Б и 1А).

Требования к защите растут от систем класса 3Б к классу 1А.

Правовые методы защиты информации



* Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 с.

Организационные методы защиты информации

Примерный комплекс мероприятий:

- определение требований к системе защиты информации;
- определение и подготовка лиц, ответственных за обеспечение безопасности информации;
- проектирование, создание и эксплуатация системы защиты информации объекта;
- научно-методологическое и документационное обеспечение работ по защите информации;
- установление мер контроля и ответственности за обеспечение всех правил защиты информации.

Технические методы защиты информации



**Торкин А.А. Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А.А. Торкин. – М.: Гелиос АРВ, 2005. – 960 с.*

Перечень нормативных документов, в той или иной мере касающихся вопросов информационной безопасности

- **Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации**
- 21 июля 1993 года N 5485-1 РОССИЙСКАЯ ФЕДЕРАЦИЯ ЗАКОН О ГОСУДАРСТВЕННОЙ ТАЙНЕ
- **Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ О персональных данных**
- 4 мая 2011 года N 99-ФЗ **РОССИЙСКАЯ ФЕДЕРАЦИЯ ФЕДЕРАЛЬНЫЙ ЗАКОН О ЛИЦЕНЗИРОВАНИИ ОТДЕЛЬНЫХ ВИДОВ ДЕЯТЕЛЬНОСТИ**
- **Федеральный закон О техническом регулировании. (в ред. Федеральных законов от 09.05.2005 № 45-ФЗ, от 01.05.2007 № 65-ФЗ, от 01.12.2007 № 309-ФЗ, от 23.07.2008 № 160-ФЗ)**
- **Закон Российской Федерации О безопасности от 5 марта 1992 г. № 2446-1 (в ред. Закона РФ от 25.12.1992 № 4235-1, Указа Президента РФ от 24.12.1993 № 2288, Федеральных законов от 25.07.2002 № 116-ФЗ, от 07.03.2005 № 15-ФЗ, от 25.07.2006 № 128-ФЗ, от 02.03.2007 № 24-ФЗ, от 26.06.2008 № 103-ФЗ)**
- **Вопросы Федеральной Службы по Техническому и Экспортному Контролю Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 (в ред. Указов Президента РФ от 22.03.2005 № 330, от 20.07.2005 № 846, от 30.11.2006 № 1321, от 23.10.2008 № 1517, от 17.11.2008 № 1625)**
- **Об утверждении перечня сведений конфиденциального характера Указ Президента Российской Федерации от 6 марта 1997 г. № 188**
- **Об утверждении перечня сведений, отнесенных к государственной тайне Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 (в ред. Указов Президента РФ от 24.01.1998 № 61, от 06.06.2001 № 659, от 10.09.2001 № 1114, от 29.05.2002 № 518, от 03.03.2005 № 243, от 11.02.2006 № 90, от 24.12.2007 № 1745, от 08.04.2008 № 460, от 30.04.2008 № 654, от 28.07.2008 № 1129, от 06.09.2008 № 1316)**

**Перечень
федеральных органов исполнительной власти, осуществляющих лицензирование**
(в редакции Постановления Правительства Российской Федерации от 26 января 2006 г. № 45 с последующими
изменениями)

ФСТЭК России

Деятельность по технической защите конфиденциальной информации

ФСТЭК России, ФСБ России

- Деятельность по разработке и (или) производству средств защиты конфиденциальной информации
- ФСБ России**
- Разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность
 - Деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)
 - Деятельность по распространению шифровальных (криптографических) средств
 - Деятельность по техническому обслуживанию шифровальных (криптографических) средств
 - Предоставление услуг в области шифрования информации
 - Разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем

Литература по основам информационной безопасности.

1. Основы информационной безопасности. Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А.Шелупанов. – М. Горячая линия – Телеком, 2006. – 544 с.
2. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов. – 4-е издание, стеритип. – М.: Горячая линия-Телеком, 2011. – 146 с.
3. Грушо А.А. Теоретические основы компьютерной безопасности: учеб. Пособие для студентов высш. учеб. заведений / А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. – М.: Издательский центр «Академия», 2009. – 272 с.
4. Куприянов А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – 2-е изд., стер. – М.: Издательский центр «Академия», 2007. – 256 с.
5. Гафнер В.В. Информационная безопасность: учеб. пособие / В.В. Гафнер. – Ростов н/Д; Феникс, 2010. – 324 с.
6. Росторгуев С.П. Основы информационной безопасности: учеб. пособие для студ. высших учебных заведений. – 2-е изд., стер. – М.: Издательский центр «Академия», 2009. – 192 с.
7. Галатенко В.А. Основы информационной безопасности: учебное пособие: / В.А. Галатенко Под редакцией академика РАН В.Б. Бетелина – 4-е изд. – М.: Интернет-Университет Информационных технологий; БИНОМ. Лаборатория знаний, 2011. – 2005 с.
8. Цирлов В.Л. Основы информационной безопасности: краткий курс /В.Л. Цирлов. – Ростов н/Д: Феникс, 2008. – 253 с.
9. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2004. – 280 с.

СПАСИБО

ЗА

ВНИМАНИЕ