Лекция

# Нормативно-правовая база в области защиты информации. Основные понятия, термины и определения.

# Структура правовой защиты информации

# Система документов в области защиты информации

**Правовые документы по технической защите информации**

Конституция Российской Федерации
Федеральные законы (Законы Российской Федерации)
Указы и распоряжения Президента Российской Федерации
Постановления Правительства Российской Федерации

**Организационно-распорядительные документы по технической защите информации**

Концепции
Положения

**Специальные нормативные документы по технической защите информации**

Государственные стандарты
Специальные нормативные документы

# Законодательная база обеспечения информационной безопасности

## Конституция Российской Федерации

*от 12 декабря 1993 г. (с изменениями и дополнениями от 9 января 1996 г. № 20; от 10 февраля 1996 г. № 173; от 9 июня 2001 г. № 679; от 25 июля 2003 г. № 841)*

Статья 1

1. Российская Федерация - Россия есть демократическое федеративное правовое государство с республиканской формой правления.

Статья 2

Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина - обязанность государства.

Статья 4

2. Конституция Российской Федерации и федеральные законы имеют верховенство на всей территории Российской Федерации.
3. Российская Федерация обеспечивает целостность и неприкосновенность своей территории.

Статья 8

2. В Российской Федерации признаются и защищаются равным образом частная, государственная, муниципальная и иные формы собственности.

Статья 15

1. Конституция Российской Федерации имеет высшую юридическую силу, прямое действие и применяется на всей территории Российской Федерации. Законы и иные правовые акты, принимаемые в Российской Федерации, не должны противоречить Конституции Российской Федерации.
2. Органы государственной власти, органы местного самоуправления, должностные лица, граждане и их объединения обязаны соблюдать Конституцию Российской Федерации и законы.
3. Законы подлежат официальному опубликованию. Неопубликованные законы не применяются. Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения.
4. Общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора.

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 этого права допускается только на основании судебного решения.

Статья 24

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.
2. Органы государственной 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

4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.
5. Гарантируется свобода массовой информации. Цензура запрещается.

# Концепция национальной безопасности РФ

*Утверждена Указом Президента РФ от 17 декабря 1997 г. № 1300 (с изменениями и дополнениями от 10.01.2000 г. № 24)*

Система взглядов на обеспечение в Российской Федерации безопасности личности, общества и государства от внешних и внутренних угроз во всех сферах жизнедеятельности.

Сформулированы важнейшие направления государственной политики Российской Федерации.

**Под *национальной безопасностью* Российской Федерации понимается безопасность ее многонационального народа как носителя суверенитета и единственного источника власти в Российской Федерации.**

**Национальные интересы России в информационной сфере:**

- соблюдение конституционных прав и свобод граждан в области получения информации и пользования ею,
- развитие современных телекоммуникационных технологий,
- защита государственных информационных ресурсов от несанкционированного доступа.

- **Серьезную опасность представляют:**

✔ стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка;

✔ разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира;

✔ нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

# Доктрина информационной безопасности РФ

*9 сентября 2000 г. № Пр-1895.*

Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ.

Развивает Концепцию национальной безопасности РФ применительно к информационной сфере.

**Служит основой для:**

- формирования государственной политики в области обеспечения информационной безопасности РФ;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности РФ;
- разработки целевых программ обеспечения информационной безопасности Российской Федерации.

# Федеральные законы в области защиты информации

| | |
|---|---|
| «О безопасности» | Закон Российской Федерации от 5 марта 1992 года № 2446-I (с изменениями и дополнениями от 1992 года № 4235-I; от 1993 года № 2288; от 2002 года № 116-ФЗ; от 2005 г. №15-ФЗ) |
| «О государственной тайне» | Закон Российской Федерации от 21 июля 1993 года № 5485-I(с изменениями и дополнениями от 6 октября 1997 г. № 131-ФЗ; от 2003 г. № 86-ФЗ; от 2003 г. № 153-ФЗ; от 2004 г. № 58-ФЗ; от 2004 г. № 122-ФЗ) |
| «О лицензировании отдельных видов деятельности» | Федеральный закон от 8 августа 2001 года № 128-ФЗ (с изменениями и дополнениями от 2002 г. №28-ФЗ, от 2002 №31-ФЗ; от 2002 г. №164-ФЗ; от 2003 г. №17-ФЗ; от 2003 г. №29-ФЗ; от 2003 г. №32-ФЗ; от 2003 г. №36-ФЗ; от 2003 г. №185-ФЗ; от 2004 г. № 127-ФЗ; от 2005 г. № 20-ФЗ) |
| Кодекс Российской Федерации об административных правонарушениях | От 30 декабря 2001 года № 195-ФЗ (выписка в части вопросов защиты информации) (с изменениями и дополнениями от 30 июня 2003 г. №86-ФЗ) |
| Уголовный кодекс Российской Федерации | От 13 июня 1996 года № 63-ФЗ (выписка в части вопросов защиты информации) (с изменениями и дополнениями от 8 декабря 2003 г. №162-ФЗ) |
| «Об электронной цифровой подписи» | Федеральный закон от 10 января 2002 года № 1-ФЗ |
| «О техническом регулировании» | Федеральный закон от 27 декабря 2002 года № 184-ФЗ (с изменениями и дополнениями от 9 мая 2005 г. № 45-ФЗ) |
| «Об информации, информационных технологиях и о защите информации» | Федеральный закон от 27 июля 2006 года № 149-ФЗ |
| «О персональных данных» | Федеральный закон от 27 июля 2006 года № 152-ФЗ |

**Закон РФ «О государственной тайне»**

*от 21 июля 1993 г. № 5485-1*

**Определяет** основные понятия, полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты.

**Дает перечень** сведений, которые могут быть отнесены к государственной тайне.

**Указывает** принципы засекречивания сведений, перечисляет сведения, не подлежащие засекречиванию.

**Устанавливает** степени секретности сведений и грифы секретности носителей этих сведений.

- **государственная тайна** - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
- **система защиты государственной тайны** - совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;

# Перечень сведений, составляющих государственную тайну

совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством

- Сведения в военной области.
- Сведения в области экономики, науки и техники.
- Сведения в области внешней политики и экономики.
- Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности.

# Сведения, не подлежащие отнесению к государственной тайне и засекречиванию

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- о фактах нарушения прав и свобод человека и гражданина;
- о размерах золотого запаса и государственных валютных резервах Российской Федерации;
- о состоянии здоровья высших должностных лиц Российской Федерации;
- о фактах нарушения законности органами государственной власти и их должностными лицами.

# Степени секретности сведений и грифы секретности носителей этих сведений

**Степень секретности** сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности РФ вследствие распространения указанных сведений.

**Гриф секретности** - реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

**особой важности**

**совершенно секретно**

**секретно**

**Закон РФ «О безопасности»** *от 5 марта 1992 г. № 2446-1*

**Закрепляет** правовые основы обеспечения безопасности личности, общества и государства, **определяет** систему безопасности и ее функции, **устанавливает** порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

**Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных»**

*от 23 октября 1992 г. № 3523-1*

Регулирует отношения, связанные с созданием, правовой охраной и использованием программ для ЭВМ и баз данных. Программы для ЭВМ и баз данных относятся к объектам авторского права.

Программам для ЭВМ предоставляется правовая охрана как произведениям литературы, а базам данных - как сборникам.

**ФЗ «Об участии в международном информационном обмене»** *от 4 июля 1996 г. № 85-ФЗ*

**Определяет** условия для эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства, защиту интересов РФ, ее субъектов и муниципальных объединений, а также физических и юридических лиц при международном информационном обмене.

**ФЗ «О техническом регулировании»** *от 27 декабря 2002 г. № 184-ФЗ*

**Регулирует** отношения, возникающие при:

- разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации;
- разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;
- оценке соответствия.

**ФЗ «Об электронной цифровой подписи»** *от 10 января 2002 г. № 1-ФЗ*

**Обеспечивает** правовые условия использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

**ФЗ «О кредитных историях»** *от 30 декабря 2004 г. № 218-ФЗ (в ред. ФЗ от 21.07.2005 N 110-ФЗ, от 24.07.2007 N 214-ФЗ)*

определяются понятие и состав кредитной истории, основания, порядок формирования, хранения и использования кредитных историй, регулируется связанная с этим деятельность бюро кредитных историй, устанавливаются особенности создания, ликвидации и реорганизации бюро кредитных историй, а также принципы их взаимодействия с источниками формирования кредитной истории, заемщиками, органами государственной власти, органами местного самоуправления и Банком России.

- ФЗ **“Об информации, информационных технологиях и о защите информации”** *от 27 июля 2006 года*

**Регулирует отношения**, возникающие при: осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий и обеспечении защиты информации.

- **информация** – сведения (сообщения, данные) независимо от формы их представления;
- **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;
- **доступ к информации** - возможность получения информации и её использования;

- Информация может являться объектом публичных, гражданских и иных правовых отношений.
- Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, *если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.*

**Классификация информации по категории доступа**

**предоставление информации** - действия, направленные на получение информации **определенным кругом лиц** или передачу информации **определенному кругу лиц**;

**распространение информации** - действия, направленные на получение информации **неопределенным кругом лиц** или передачу информации **неопределенному кругу лиц**;

## Классификация информации в зависимости от порядка её предоставления или распространения

**ИНФОРМАЦИЯ**

- Информация, свободно распространяемая
- Информация, предоставляемая по соглашению лиц, участвующих в соответствующих отношениях
- Информация, распространение которой в РФ ограничивается или запрещается
- Информация, которая в соответствии с федеральными законами подлежит предоставлению или распространению

# Обладатель информации

**Права:**

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

**Обязанности:**

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

# Не может быть ограничен доступ

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

**ФЗ «О персональных данных»** *от 27 июля 2006 г. № 152-ФЗ*

**Регулирует отношения**, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, . . . физическими лицами с использованием средств автоматизации или без использования таких средств, . . .

**Целью настоящего ФЗ** является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

- ***Персональные данные*** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- ***Оператор*** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;
- ***Информационная система*** персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;
- ***Конфиденциальность персональных данных*** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;
- ***Общедоступные персональные данные*** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Постановление Правительства РФ "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных”** *от 17 ноября 2007 г. N 781*

В соответствии со статьей 19 ФЗ "О персональных данных”:

- Вводит в действие Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных.
- Постановляет ФСБ и ФСТЭК в пределах своей компетенции в 3-месячный срок разработать нормативные правовые акты и методические документы, необходимые для выполнения требований, предусмотренных Положением, утвержденным настоящим постановлением.

**Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных.**

**Устанавливает** требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

**Информационная система персональных данных** - совокупность персональных данных, содержащихся в базах данных, а также информационных и технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

# ФЗ РФ «О коммерческой тайне». № 98-ФЗ от 29.07.2004 г.

- ***Коммерческая тайна*** - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.
- ***Информация, составляющая коммерческую тайну*** – научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.
- ***Режим коммерческой тайны*** – правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности.
- ***Обладатель информации, составляющей коммерческую тайну*** – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайне.
- ***Доступ к информации, составляющей коммерческую тайну*** - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.
- ***Разглашение информации, составляющей коммерческую тайну*** – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, или иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

**ФЗ «О связи»** *от 7 июля 2003 г. N 126-ФЗ*

**Устанавливает** правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

# Указы и распоряжения Президента Российской Федерации

| | |
|---|---|
| Об утверждении Концепции национальной безопасности Российской Федерации | Указ Президента Российской Федерации от 1997 года № 1300 (с изменениями и дополнениями от 10 января 2000 года № 24) |
| Вопросы Федеральной службы по техническому и экспортному контролю | Указ Президента Российской Федерации от 16 августа 2004 года № 1085 (с изменениями и дополнениями от 2005 г. № 330; от 2005 г. №846; от 2006 г. № 1321) |
| Вопросы Межведомственной комиссии по защите государственной тайны | Указ Президента Российской Федерации от 2004 г. № 1286 |
| Об утверждении Перечня сведений, отнесенных к государственной тайне | Указ Президента Российской Федерации от 1995 года № 1203 (с изменениями и дополнениями от 1998 года № 61; от 2001 года № 659; от 2001 года № 1114; от 2002 года № 518; от 2005 г. № 243; от 2006 г. № 90) |
| Об утверждении Перечня должностных лиц органов государственной власти Российской Федерации, наделенных полномочиями по отнесению сведений к государственной тайне | Распоряжение Президента Российской Федерации от 2005 г. № 151-рп |
| Об утверждении Перечня сведений конфиденциального характера | Указ Президента Российской Федерации от 1997 года № 188 |
| О составе межведомственного коллегиального органа - коллегии Федеральной службы по техническому и экспортному контролю | Распоряжение Президента Российской Федерации от 2005 г. № 298-рп |
| Об учреждении флага Федеральной службы по техническому и экспортному контролю | Указ Президента Российской Федерации от 2005 г. № 1364 |
| О реестре должностей федеральной государственной гражданской службы | Указ Президента Российской Федерации от 2005 г. № 1574 |

**Постановление Совета Министров Правительства РФ № 912-51**
*от 15 сентября 1993 г.*

Вводит соответствующее Положение «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам».

**Указ Президента РФ «Вопросы Федеральной службы по техническому и экспортному контролю»** *от 16 августа 2004 г. № 1085.*

Вводит в действие Положение «О Федеральной службе по техническому и экспортному контролю» в котором определяются полномочия и организация деятельности ФСТЭК.

**Постановление Правительства РФ «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»** *от 3 ноября 1994 г. № 1233.*

**Постановление Правительства РФ «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»** *от 29 декабря 2007 г. N 957*

Определяет порядок лицензирования деятельности по распространению шифровальных (криптографических) средств, осуществляемой юридическими лицами и индивидуальными предпринимателями.

**Указ Президента РФ «Об утверждении перечня сведений, отнесенных к государственной тайне»** *от 30 ноября 1995 года № 1203*

В соответствии со статьей 4 Закона РФ «О государственной тайне» ***утверждается*** перечень сведений, отнесенных к государственной тайне.

Правительству РФ предписывается организовать работу по приведению действующих нормативных актов в соответствие с Перечнем сведений, отнесенных к государственной тайне.

**Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера»** *от 6 марта 1997 г. № 188*.

**Утверждает перечень сведений конфиденциального характера**

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

# Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»

*от 17 марта 2008 г. № 351*

В целях обеспечения информационной безопасности РФ при использовании информационно-телекоммуникационных сетей (И-ТС), позволяющих осуществлять передачу информации через гос.границу РФ, в том числе при использовании международной компьютерной сети "Интернет", постановляет:

а) подключение информационных систем (ИС), И-ТС и средств вычислительной техники (СВТ), применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие гос.тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к И-ТС, позволяющим осуществлять передачу информации через государственную границу РФ, в том числе к международной компьютерной сети "Интернет" не допускается;

б) при необходимости подключения ИС, И-ТС и СВТ, указанных в подпункте "а" настоящего пункта, к И-ТС международного информационного обмена (МИО) такое подключение производится только с использованием специально предназначенных для этого средств защиты информации (СЗИ), в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством РФ порядке сертификацию в ФСБ РФ и (или) получивших подтверждение соответствия в ФСТЭК. Выполнение данного требования является обязательным для операторов ИС, владельцев И-ТС и (или) СВТ;

**Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»**
*от 17 марта 2008 г. № 351*

в) государственные органы в целях защиты общедоступной информации, размещаемой в И-ТС МИО, используют только СЗИ, прошедшие в установленном законодательством РФ порядке сертификацию в ФСБ РФ и (или) получившие подтверждение соответствия в ФСТЭК;

г) размещение технических средств, подключаемых к И-ТС МИО, содержащие сведения, составляющие гос.тайну, осуществляется только при наличии сертификата, разрешающего эксплуатацию таких технических средств в указанных помещениях. Финансирование расходов, связанных с размещением технических средств в указанных помещениях федеральных органов гос. власти, осуществляется в пределах бюджетных ассигнований, предусмотренных в федеральном бюджете на содержание этих органов.

**Признать утратившим силу Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена»**
от 12 мая 2004 г. № 611.

# Постановление Правительства РФ «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

*от 17.11.2007 № 781*

Персональными данными гражданина, подлежащим защите, признается любая информация, относящаяся к физическому лицу, ***в том числе*** его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к ним, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Обмен персональными данными при их обработке в информационных системах (ИС) осуществляется по защищенным каналам связи.

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

При обработке персональных данных в ИС должно быть обеспечено:

- предотвращение несанкционированного доступа к данным или передачи их лицам, не имеющим права доступа;
- своевременное обнаружение фактов несанкционированного доступа;
- недопущение воздействия средства обработки данных, в результате которого они могут быть может быть нарушено их функционирование;
- возможность незамедлительного восстановления данных, измененных или уничтоженных при несанкционированном доступе;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

# Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

*от 15 сентября 2008 г. N 687 г.*

В целях реализации ФЗ "О персональных данных" Правительство РФ ***постановляет*:**

1. Утвердить прилагаемое Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.
2. Федеральным органам исполнительной власти в ***месячный срок*** привести свои акты по вопросам обработки персональных данных, осуществляемой без использования средств автоматизации, в соответствие с настоящим постановлением.
3. Настоящее постановление вступает в силу по истечении одного месяца со дня его официального опубликования.

**I. Общие положения**

**II. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации**

**III. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации**

13. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.
14. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.
15. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

# Положения по защите информации

| | |
|---|---|
| Положение о Федеральной службе по техническому и экспортному контролю | Утверждено Указом Президента Российской Федерации от 16 августа 2004 года № 1085 |
| Положение о Межведомственной комиссии по защите государственной тайны | Утверждено Указом Президента Российской Федерации от 6 октября 2004 г. № 1286 |
| Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны | Утверждено постановлением Правительства Российской Федерации от 15 апреля 1995 года № 333 (с изменениями и дополнениями от 23 апреля 1996 г. № 509; от 30 апреля 1997 г. № 513; от 29 июля 1998 г. № 854; от 3 октября 2002 г. № 731; от 17 декабря 2004 г. № 807) |
| Положение о лицензировании образовательной деятельности | Утверждено постановлением Правительства Российской Федерации от 18 октября 2000 года № 796 (с изменениями и дополнениями от 3 октября 2002 г. №731) |
| Положение о государственном лицензировании деятельности в области защиты информации | Решение Гостехкомиссии России и ФАПСИ от 27 апреля 1994 года № 10 (с дополнениями от 24 июня 1997 года № 60) |
| Положение о лицензировании разработки авиационной техники, в том числе авиационной техники двойного назначения | Утверждено постановлением Правительства Российской Федерации от 27 мая 2002 года № 346 (с изменениями и дополнениями от 3 октября 2002 года № 731) |
| Положение о лицензировании производства авиационной техники, в том числе авиационной техники двойного назначения | Утверждено постановлением Правительства Российской Федерации от 27 мая 2002 года № 346 (с изменениями и дополнениями от 3 октября 2002 года № 731) |
| Положение о лицензировании ремонта авиационной техники, в том числе авиационной техники двойного назначения | Утверждено постановлением Правительства Российской Федерации от 27 мая 2002 года № 346 (с изменениями и дополнениями от 3 октября 2002 года № 731) |

# Положения по защите информации

| | |
|---|---|
| Положение о лицензировании производства оружия и основных частей огнестрельного оружия | Утверждено постановлением Правительства Российской Федерации от 2002 года № 455 (с изменениями и дополнениями от 2002 года № 731) |
| Положение о лицензировании деятельности в области вооружения и военной техники | Утверждено постановлением Правительства Российской Федерации от 2002 года № 456 (с изменениями и дополнениями от 2002 года № 731) |
| Положение о лицензировании разработки и производства боеприпасов | Утверждено постановлением Правительства Российской Федерации от 2002 года № 467 (с изменениями и дополнениями от 2002 года № 731) |
| Положение о лицензировании утилизации боеприпасов | Утверждено постановлением Правительства Российской Федерации от 2002 года № 467 (с изменениями и дополнениями от 2002 года № 731) |
| Положение о лицензировании производства пиротехнических изделий | Утверждено постановлением Правительства Российской Федерации от 2002 года № 467 (с изменениями и дополнениями 2002 года № 731) |
| Положение о лицензировании деятельности по распространению пиротехнических изделий IV и V классов в соответствии с государственным стандартом | Утверждено постановлением Правительства Российской Федерации от 2002 года № 467 (с изменениями и дополнениями от 2002 года № 731) |
| Положение о лицензировании деятельности по технической защите конфиденциальной информации | Утверждено постановлением Правительства Российской Федерации от 15 августа 2006 г. № 504 |
| Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации | Утверждено постановлением Правительства Российской Федерации от 31 августа 2006 г. № 532 |
| Положение о лицензировании деятельности по международному информационному обмену | Утверждено постановлением Правительства Российской Федерации от 1998 года № 564 (с изменениями и дополнениями от 2002 года № 731) |

# Положения по защите информации

| | |
|---|---|
| Положение о сертификации средств защиты информации | Утверждено постановлением Правительства Российской Федерации от 1995 года № 608 (с изменениями и дополнениями от 1996 г. № 509; от 1999 г. № 342; от 2004 г. № 808) |
| Положение о сертификации средств защиты информации по требованиям безопасности информации | Утверждено приказом председателя Гостехкомиссии России от 1995 года № 199 |
| Положение по аттестации объектов информатизации по требованиям безопасности информации | Утверждено председателем Гостехкомиссии России от 25 ноября 1994 года |
| Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации | Решение председателя Гостехкомиссии России от 25 ноября 1994 года |
| Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации | Утверждено приказом председателя Гостехкомиссии России от 5 января 1996 года № 3 |
| Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации | Утверждено приказом председателя Гостехкомиссии России от 5 января 1996 года № 3 |
| Типовое положение об испытательной лаборатории | Утверждено приказом председателя Гостехкомиссии Россииот 25 ноября 1994 г. |
| Положение о размещении и использовании на территории Российской Федерации, на континентальном шельфе и в исключительной экономической зоне Российской Федерации иностранных технических средств наблюдения и контроля | Утверждено постановлением Правительства Российской Федерации от 29 августа 2001 года № 633 |
| Положение о лицензировании деятельности по изготовлению защищенной от подделок полиграфической продукции, в том числе бланков ценных бумаг, а также торговли указанной продукцией | Утверждено постановлением Правительства Российской Федерации от 11 ноября 2002 г. № 817 (с изменениями и дополнениями от 9 декабря 2002 г. №745; от 18 мая 2005 г. № 309) |

# Нормативная база обеспечения информационной безопасности

**ГОСТ СССР 24.701-86 Единая система стандартов автоматизированных систем управления.** Надежность автоматизированных систем управления. Основные положения.

**ГОСТ Р 50739-95 Средства вычислительной техники.** Защита от несанкционированного доступа к информации. Общие технические требования.

**ГОСТ Р 50922-96 Защита информации.** Основные термины и определения

**ГОСТ Р 51188-98 Защита информации.** Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

**ГОСТ Р 51275-99 Защита информации.** Объекты информатизации. Факторы воздействующие на информацию. Общие положения.

**ГОСТ Р 51241-98 Средства и системы контроля и управления доступом.** Классификация. Общие технические требования. Методы испытаний.

ГОСТ Р ИСО 15489-1— 2007 **Система стандартов по информации**, библиотечному и издательскому делу . Управление документами. Общие требования

**ГОСТ Р 51583-2000. Защита информации.** Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.

**ГОСТ Р 51624-2000. Защита информации.** Автоматизированные системы в защищённом исполнении. Общие требования.

**ГОСТ Р 52069.0-2003 Защита информации.** Система стандартов. Основные положения.

**ГОСТ Р 51901.1-2002 Управление надежностью.** Анализ риска технологических систем.

**ГОСТ Р 51901.5-2005 Менеджмент риска.** Руководство по применению методов анализа надежности.

**ГОСТ Р 52447-2005 Защита информации.** Техника защиты информации. Номенклатура показателей качества.

**ГОСТ Р 52478-2005 Защита информации.** Обеспечение безопасности сетей электросвязи. Общие положения.

**ГОСТ Р 34.10 -2001 Информационная технология.** Криптографическая защита. Процессы формирования и проверки электронной цифровой подписи.

**ГОСТ Р 51898-2002 Аспекты безопасности.** Правила включения в

**ГОСТ Р ИСО/МЭК ТО 13335-1-2006 Методы и средства обеспечения безопасности** *Часть 1* Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

**ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Методы и средства обеспечения безопасности** *Часть 3* Методы менеджмента безопасности информационных технологий

**ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Методы и средства обеспечения безопасности** *Часть 4* Выбор защитных мер

**ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Методы и средства обеспечения безопасности** *Часть 5* Руководство по менеджменту безопасности сети

**ГОСТ ИСО/МЭК 15408-1-2002.** Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

**ГОСТ ИСО/МЭК 15408-2-2002.** Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий Часть 2. Функциональные требования безопасности.

**ГОСТ Р ИСО/МЭК 15408-3-2002.** Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

**ГОСТ Р ИСО/МЭК 17799-2005.** Практические правила управления информационной безопасностью

**BS 7799-1** – (Code of Practice for Information Security Management) Практические правила управления информационной безопасностью.

**BS 7799-2** - Information Security management – specification for information security management systems (Спецификация системы управления информационной безопасностью). Системы управления информационной безопасностью. Спецификация и руководство по применению.

ISO/IEC 27001:2005 - Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.

**ISO 27002** Практические правила управления информационной безопасностью. *Выпуск стандарта запланирован на 2006-2007 г.*

**ISO 27003** Руководство по внедрению системы управления ИБ. *Выпуск стандарта запланирован на 2007 г.*

**ISO 27004** Измерение эффективности системы управления ИБ. *Выпуск стандарта запланирован на 2007 г.*

**ISO 27005** Управление рисками ИБ.
*Выпуск стандарта запланирован на 2007 г.*

# Кодекс Российской Федерации об административных правонарушениях
*от 30 декабря 2001 года № 195-ФЗ*

**Статья 13.11. Нарушение порядка сбора, хранения и использования или распространения персональных данных.**

- на граждан в размере от 3 до 5 МРОТ;
- для должностных лиц от 5 до 10 МРОТ;
- для юридических лиц от 50 до 100 МРОТ.

**Статья 13.12. Нарушение правил защиты информации.**

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну).

- на граждан в размере от 3 до 5 МРОТ;
- на должностных лиц - от 5 до 10 МРОТ;
- на юридических лиц - от 50 до 100 МРОТ.

2. **Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну).**

**Административный штраф:**

- на граждан в размере от 5 до 10 МРОТ с конфискацией несертифицированных средств защиты информации или без таковой;
- на должностных лиц - от 10 до 20 МРОТ;
- на юридических лиц - от 100 до 200 МРОТ с конфискацией несертифицированных средств защиты информации или без таковой.

**3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей ГТ, созданием средств, предназначенных для ЗИ, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей ГТ.**

**Административный штраф:**

- на должностных лиц в размере от 20 до 30 МРОТ;
- на юридических лиц - от 150 до 200 МРОТ.

**4. Использование несертифицированных средств, предназначенных для ЗИ, составляющей ГТ.**

**Административный штраф:**

- на должностных лиц в размере от 30 до 40 МРОТ;
- на юридических лиц - от 200 до 300 МРОТ с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

**Статья 13.13. Незаконная деятельность в области защиты информации.**

1. **Занятие видами деятельности в области ЗИ (за исключением информации, составляющей ГТ) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна).**

**Административный штраф:**

- на граждан в размере от **5 до 10 МРОТ** с конфискацией средств защиты информации или без таковой;
- на должностных лиц - от 20 до 30 МРОТ с конфискацией средств защиты информации или без таковой;
- на юридических лиц - от 100 до 200 МРОТ с конфискацией средств защиты информации или без таковой.

2. Занятие видами деятельности, связанной с использованием и ЗИ, составляющей ГТ, созданием средств, предназначенных для ЗИ, составляющей ГТ, осуществлением мероприятий и (или) оказанием услуг по ЗИ, составляющей ГТ без лицензии.

**Административный штраф:**

- на должностных лиц в размере от 40 до 50 МРОТ;
- на юридических лиц - от 300 до 400 МРОТ с конфискацией созданных без лицензии средств защиты информации, составляющей ГТ, или без таковой.

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.

**Административный штраф:**

- на граждан в размере от 5 до 10 МРОТ;
- на должностное лицо - от 40 до 50 МРОТ.

# Уголовный кодекс Российской Федерации
*от 13 июня 1996 года № 63-ФЗ*

**Статья 272. Неправомерный доступ к компьютерной информации.**

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

**Штраф:**

- в размере от 200 до 500 МРОТ или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев, либо исправительными работами на срок от 6 месяцев до 1 года, либо лишением свободы на срок до 2 лет.

**2.** То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

**Штраф:**

- в размере от 500 до 800 МРОТ,
- в размере заработной платы или иного дохода осужденного за период от 5 до 8 месяцев.

**Исправительными работами** на срок от 1 года до 2 лет.

**Арест** на срок от 3 до 6 месяцев.

**Лишение свободы** на срок до 5 лет.

**Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.**

**1.** Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.

**Лишение свободы** на срок до 3 лет со штрафом в размере от 200 до 500 МРОТ или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

**2.** Те же деяния, повлекшие по неосторожности тяжкие последствия.

**Лишение свободы** на срок от 3 до 7 лет.

**Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.**

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред

**Лишение права занимать определенные должности** или заниматься определенной деятельностью на срок до 5 лет,

**Либо обязательными работами** на срок от 180 до 240 часов,

**Либо ограничением свободы** на срок до 2 лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия.

**Лишение свободы** на срок до 4 лет.

**Собирание сведений,** составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом - наказывается штрафом в размере до **80000 р.** или в размере заработной платы или иного дохода осужденного за период **от 1 до 6 месяцев** либо лишением свободы на срок **до двух лет.**

**Незаконные разглашение или использование сведений,** составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, - наказываются штрафом в размере до **120000** рублей или в размере заработной платы или иного дохода осужденного за период **до одного года** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок **до 3 лет** либо лишением свободы на срок **до 3 лет.**

**Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности** - наказываются штрафом в размере до **200000 р.** или в размере заработной платы или иного дохода осужденного за период **до 18 месяцев** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок **до трех лет** либо лишением свободы на срок **до пяти лет.**

**Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия** - наказываются лишением свободы на срок **до 10 лет.**

# ФЗ «О внесении изменений в Трудовой кодекс РФ...» *от 30.06.2006 № 90-ФЗ*

- Приравнял разглашение персональных данных другого работника, ставших известными в связи с исполнением служебных обязанностей, к разглашению охраняемой законом тайны. *Возможно увольнение сотрудника. Раздел «Прекращение трудового договора» ТК.*
- Установленный ст. 391 перечень индивидуальных трудовых споров, подлежащих рассмотрению непосредственно в судах, дополнен спорами по заявлениям работников о неправомерных действиях (бездействии) работодателя при обработке и защите персональных данных работника. *Раздел «Рассмотрение и разрешение индивидуальных трудовых споров».*
- Работодатель получает право уволить служащего, допустившего утечку персональных данных других сотрудников компании.
- Однако сам работник может подать в суд на свое предприятие, если оно не заботится о приватных сведениях персонала, как того требует закон.

# Нормативно-методические и методические документы

**Положение по аттестации объектов информатизации по требованиям безопасности информации,** *утверждено председателем Гостехкомиссии России 25 ноября 1994 г.*

Устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

**Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации.** *утверждено председателем Гостехкомиссии России 25 ноября 1994 г.*

РД Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. *Гостехкомиссия России, 1992.*

РД Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. *Гостехкомиссия России, 1992.*

РД Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. *Гостехкомиссия России, 1992.*

РД Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. *Гостехкомиссия России, 1992.*

РД Защита от несанкционированного доступа к информации. Термины и определения. *Гостехкомиссия России, 1992.*

РД Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. *Гостехкомиссия России, 1997.*

РД Защита информации. Специальные защитные знаки. Классификация и общие требования. *Гостехкомиссия России, 1997.*

РД Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. *Утвержден приказом Гостехкомиссии России от 4 июня 1999 г. № 114.*

РД Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. *Утвержден приказом Гостехкомиссии России от 19 июня 2002 г. № 187 (часть 1, часть 2, часть 3).*

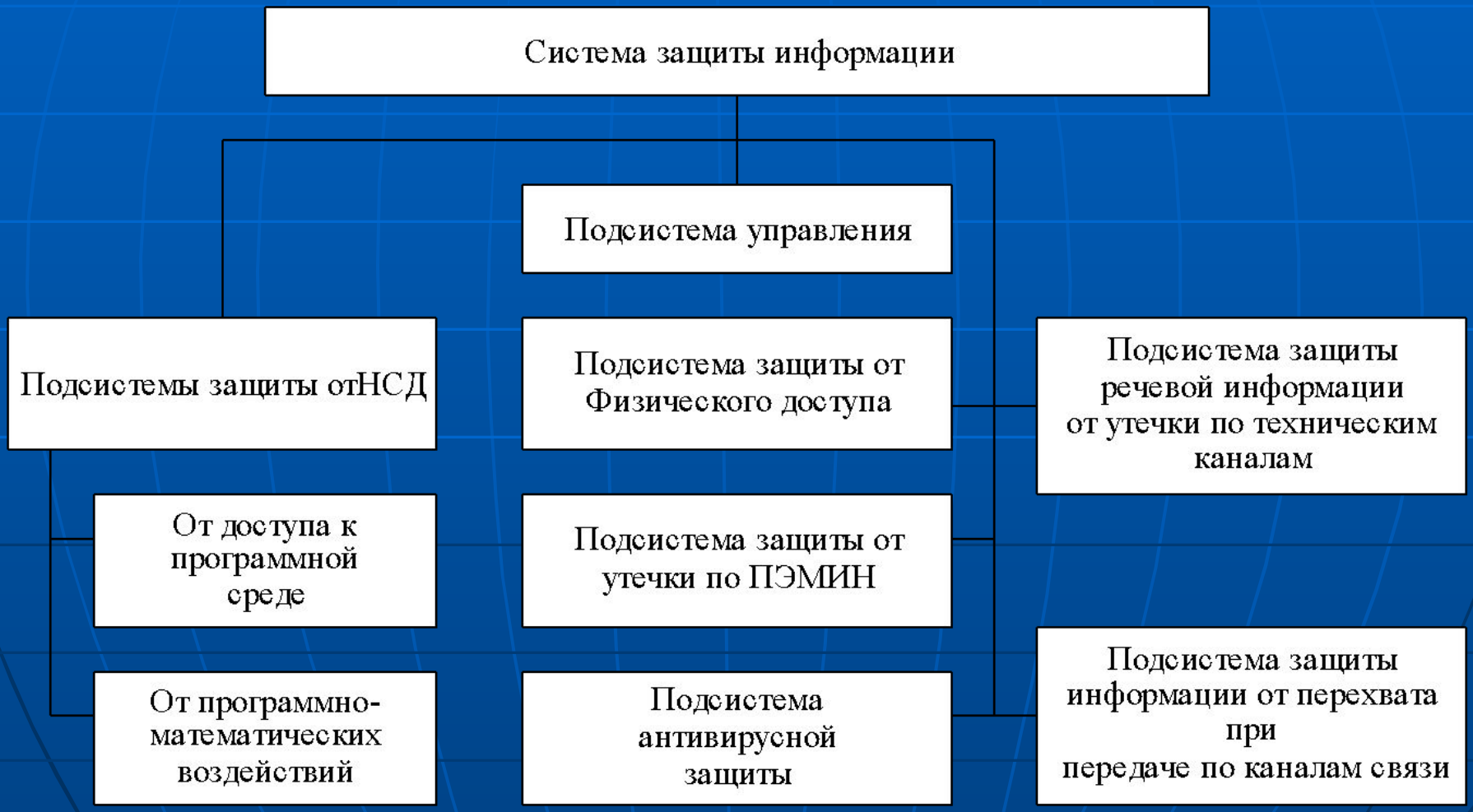
«Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации», *Гостехкомиссия России, Москва, 2002.*[*]

**РД Методические рекомендации по технической защите информации, составляющей коммерческую тайну.** *2007.*

1. Основные понятия и сокращения.
2. Понятие коммерческой тайны.
3. Порядок определения сведений, составляющих КТ.
4. Категорирование объектов информатизации по уровням защищенности и группам коммерческой ценности информации.
5. Методические рекомендации по общему порядку организации ЗИ, составляющей КТ, на ОИ.
6. Методические рекомендации по порядку выявления актуальных угроз безопасности информации, составляющей коммерческую тайну.

7. Рекомендации по применению мер и средств технической защиты информации, составляющей коммерческую тайну.

7.1. Общие рекомендации.



«Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации», *Гостехкомиссия России, Москва, 2002.*[*]

«Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам», *Гостехкомиссия России, Москва, 2002.*[*]

«Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах», *Гостехкомиссия России, Москва, 2002.*[*]

НМД «Специальные требования и рекомендации по технической защите конфиденциальной информации». *Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282.*

Приказ ФСТЭК России «Об утверждении форм документов, используемых ФСТЭК России в процессе лицензирования деятельности по технической защите конфиденциальной информации и деятельности по разработке и (или) производству средств защиты конфиденциальной информации» *от 7 июля 2006 г. № 222, (зарегистрирован Минюстом России 27 июля 2006 г., регистрационный № 8114).*

** - Документ ограниченного распространения*

# Стандарты

**ГОСТ 17168-82.** Фильтры электронные октавные и третьоктавные. Общие технические требования и методы испытаний.

**ГОСТ 12.1.003-83.** Система стандартов безопасности труда. Шум. Общие требования безопасности.

**ГОСТ 21552-84.** Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортировка и хранение.

**ГОСТ 12.1.050-86.** ССБТ. Методы измерения шума на рабочих местах.

**ГОСТ 27296-87.** Защита от шума в строительстве. Звукоизоляция ограждающих конструкций. Методы измерений.

**ГОСТ 27201-87.** Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования.

**ГОСТ 34.201-89.** Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.

**ГОСТ 34.602-89.** Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

**ГОСТ 28806-90.** Качество программных средств. Термины и определения.

**ГОСТ 34.003-90.** Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

**ГОСТ 2.503-90.** ЕСКД. Правила внесения изменений.

**ГОСТ 34.601-90.** Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

**ГОСТ 29216-91.** Совместимость технических средств электромагнитная. Радиопомехи индустриальные от оборудования информационной техники. Нормы и методы испытаний.

**ГОСТ 34.603-92.** Информационная технология. Виды испытаний автоматизированных систем.

**ГОСТ Р ИСО 9127-94.** Системы обработки информации. Документация пользователя и информация на упаковке для потребительских программных пакетов.

**ГОСТ 30373-95/ГОСТ Р 50414-92.** Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний.

**ГОСТ Р 50739-95.** Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

**ГОСТ Р 50752-95.** Информационная технология. Защита информации от утечки за счёт побочных электромагнитных излучений при её обработке средствами вычислительной техники. Методы испытаний.

**ГОСТ Р 50922-96.** Защита информации. Основные термины и определения.

**ГОСТ Р ИСО 9001-96.** Системы качества. Модель обеспечения качества при проектировании, разработке, производстве, монтаже и обслуживании.

**ГОСТ Р ИСО 9002-96.** Системы качества. Модель обеспечения качества при производстве, монтаже и обслуживании.

**ГОСТ Р ИСО 9003-96.** Системы качества. Модель обеспечения качества при окончательном контроле и испытаниях.

**ГОСТ Р 50922-96.** Защита информации. Основные термины и определения.

**ГОСТ Р 50923-96.** Дисплеи. Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения.

**ГОСТ 22505-97.** Совместимость технических средств электромагнитная. Радиопомехи индустриальные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний.

**ГОСТ Р 51188-98.** Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

**ГОСТ Р 51171-98.** Качество служебной информации. Правила предъявления информационных технологий на сертификацию.

**ГОСТ Р 51275-99.** Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

**ГОСТ Р 51320-99.** Совместимость технических средств электромагнитная. Радиопомехи индустриальные. Методы испытаний технических средств - источников индустриальных радиопомех.

**ГОСТ Р 51319-99.** Совместимость технических средств электромагнитная. Приборы для измерения индустриальных радиопомех. Технические требования и методы испытаний.

**ГОСТ Р 51583-2000.** Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения, (дсп).

**ГОСТ Р 51624-2000.** Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования, (дсп).

**ГОСТ Р 50628-2000.** Совместимость -технических средств электромагнитная. Устойчивость машин электронных вычислительных персональных к электромагнитным помехам. Требования и методы испытаний.

**ГОСТ Р ИСО 9000-2001.** Системы менеджмента качества. Основные положения и словарь.

**ГОСТ Р ИСО 9001-2001.** Системы менеджмента качества. Общие требования.

**ГОСТ Р ИСО 9004-2001.** Системы менеджмента качества. Рекомендации по улучшению качества.

**ГОСТ Р 50948-2001.** Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности.

**ГОСТ Р 50949-2001.** Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности.

**ГОСТ ИСО/МЭК 15408-1-2002.** Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

**ГОСТ ИСО/МЭК 15408-2-2002.** Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий Часть 2. Функциональные требования безопасности.

**ГОСТ ИСО/МЭК 15408-3-2002.** Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

**РД 50-682-89.** Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные

# На сайте Федерального агентства по техническому регулированию и метрологии размещены

| | |
|---|---|
| ГОСТ Р 52447-2005 | Защита информации. Техника защиты информации. Номенклатура показателей качества |
| ГОСТ Р 52069.0-2003 | Защита информации. Система стандартов. Основные положения |
| ГОСТ Р 50922-2006 | Защита информации. Основные термины и определения |
| ГОСТ Р 52448-2005 | Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения |
| ГОСТ Р 51275-2006 | Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения |
| ГОСТ Р 52633-2006 | Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации |
| ГОСТ Р 52863-2007 | Защита информации. Автоматизированные системы в защищенном исполнении испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования |
| ГОСТ Р 34.10-2001 | Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи |
| ГОСТ 34.311-95 | Информационная технология. Криптографическая защита информации. Функция хэширования |
| ГОСТ Р 34.11-94 | Информационная технология. Криптографическая защита информации. Функция хэширования |
| ГОСТ Р 51188-98 | Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство |

# Спасибо за внимание