



ГУАП

guap.ru

## Вводная лекция по дисциплине:

«Организационное и  
правовое обеспечение  
информационной  
безопасности»

Доцент кафедры №33  
Ерышев Вадим Георгиевич  
Кандидат технических наук

## Цели дисциплины «Организационное и правовое обеспечение информационной безопасности»:



01

Рассмотреть, систематизировать основное правовое обеспечение в области ИБ: нормативные правовые акты (федеральные законы, постановления правительства, указы президента), методические документы регуляторов, международные и национальные стандарты.



02

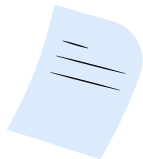
Рассмотреть, систематизировать основное организационное обеспечение в области ИБ (концепции, политики, положения, регламенты, инструкции, приказы, планы, отчеты).



# Вопросы:



1. Основные понятия и определения
2. Нормативные правовые акты, методические документы, международные и национальные стандарты в области ИБ





## Деятельность по обеспечению ИБ

**Законодательно-  
правовое обеспечение**



**Программно-техническое  
обеспечение**



**Организационное  
обеспечение**





**Безопасность информации** - состояние защищенности информации, характеризующееся способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.



**Доступ к информации, составляющей коммерческую тайну, (санкционированный)** - возможность получения и использования информации, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.



**Несанкционированный доступ к информации, составляющей коммерческую тайну** - доступ к информации, составляющей коммерческую тайну, с нарушением установленных обладателем коммерческой информации прав или правил доступа к защищаемой информации с помощью программных или программно-технических средств.



**Информация** - сведения (сообщения, данные) независимо от формы их представления.



\*\*\*\*\*

**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.



**Информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.



**Информационная безопасность** – это процесс обеспечения конфиденциальности, целостности и доступности информации.



**Информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.



**Информационно-телекоммуникационная сеть** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.



**Защищаемые помещения (ЗП)** - помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения мероприятий (совещаний, конференций, переговоров и т.п.), на которых обсуждаются вопросы, связанные с коммерческой тайной.



**Коммерческая тайна (КТ)** - 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.



**Конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.



**Объект информатизации** - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объектов информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения или объекты, предназначенные для ведения конфиденциальных переговоров.





**Система защиты информации, составляющей коммерческую тайну** - совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно - распорядительными и нормативными документами в области защиты информации, составляющей коммерческую тайну.



**Технический канал утечки информации** - совокупность источника информативного сигнала (человек, техническое средство и т.д.), средства регистрации информативного сигнала и физической среды, в которой распространяется информационный сигнал.



**Угроза безопасности информации** - совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее.



**Режим коммерческой тайны** - правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по обеспечению ее конфиденциальности.





Согласно **Федеральному закону** «Об информации, информационных технологиях и защите информации» от 27.06.2006 № 149-ФЗ:

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

Согласно **ГОСТ Р 50922–2006** «Защита информации. Основные термины и определения»:

**ЗИ** - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

- **Зона2 (R2)** - пространство вокруг ОТСС, на границе и за пределами которого напряженность электромагнитного поля информативного сигнала не превышает нормированного значения (R2 является параметром технического средства, характеризующим защищенность обрабатываемой им информации от утечки).
- **Зона1 (R1)** - пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в ВТСС, а также в посторонних проводах и линиях передачи информации, имеющих выход за пределы КЗ, не превышает нормированного значения ( $r1$  – сосредоточенные,  $r1'$ -распределенные случайные антенны).
- **Контролируемая зона (КЗ)** - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание работников и посетителей организации, а также транспортных, технических и иных материальных средств.
- **Основные технические средства и системы (ОТСС)** - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.
- **Вспомогательные технические средства и системы (ВТСС)** - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

# Нормативные правовые акты, методические документы, международные и национальные стандарты в области ИБ

**Информация** – сведения (сообщения, данные) независимо от формы их представления

## Ограниченного доступа

Государственная тайна

Служебная тайна

Коммерческая тайна

Персональные данные

## Общедоступная

Сведения о  
деятельности  
Правительства РФ и  
федеральных органов  
власти, обязательные  
для размещения в ИТС  
Интернет

АС

ГИС

ИСПДн

ИСОП

# Структура нормативных правовых актов в области ИБ

## Правовая защита информации

Специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе

### Международное право

- Декларации
- Патенты
- Авторские права
- Лицензии


### Внутригосударственное право

#### Государственные


- Конституция
- Законы
- Указы
- Постановления

#### Ведомственные


- Приказы
- Руководства
- Положения
- Инструкции и т.д.



**Первый блок** - конституционное законодательство. Нормы, касающиеся вопросов информатизации и ЗИ, входят в него как составные элементы.



**Второй блок** - общие законы, кодексы которые включают нормы по вопросам информационных технологий и ИБ.



**Третий блок** - законы об организации управления, касающиеся отдельных структур хозяйства, экономики, системы государственных органов и определяющие их статус. Они включают отдельные нормы по вопросам ЗИ. Наряду с общими вопросами информационного обеспечения и ЗИ конкретного органа эти нормы должны устанавливать его обязанности по формированию, актуализации и безопасности информации, представляющей общегосударственный интерес.



**Четвертый блок** - специальные законы, полностью относящиеся к конкретным сферам отношений, отраслям хозяйства, процессам.



**Пятый блок** - законодательство субъектов Российской Федерации, касающееся защиты информации.



**Шестой блок** - подзаконные нормативные акты по защите информации.



**Седьмой блок** - правоохранительное законодательство России, содержащее нормы об ответственности за правонарушения в сфере информатизации.

## Информационные ресурсы с правовыми актами по правовой защите информации



<http://www.fstec.ru>

<http://www.fsb.ru>

<http://rkn.gov.ru/personal-data/>


<http://www.garant.ru>

<http://www.consultant.ru>

<http://www.gost.ru/wps/portal>

<http://www.abiss.ru/doc>






# ФСТЭК России

Федеральная служба по техническому и экспортному контролю

ГлавнаяКарта сайтаОбновленияТекст для поиска

RUEN

КонтактыИнформацияДеятельность**Документы**Техническая защита информацииЭкспортный контрольЛицензированиеКадровое обеспечение

Противодействие коррупцииТерриториальные органы**ГНИИИ ПТЗИ ФСТЭК России**ТК 362

Главная / Документы / Техническая защита информации

Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации

Категории, содержащие информационные материалы:

**Законы** 3

**Указы** 5

**Постановления** 1

**Приказы** 7

**Положения** 1

**Специальные нормативные документы** 11

**Национальные стандарты** 1



Если заметили ошибку в тексте, выделите ее курсором мыши и нажмите Ctrl + Enter

#### Навигация

Главная

Карта сайта

#### Ссылки

Портал госуслуг

Открытые данные

Версия для слабовидящих

#### О сайте

Об использовании информации сайта

Об использовании персональных данных пользователей информации

О разработке и администрировании сайта



- **Федеральный закон** от 28 декабря 2010 № 390-ФЗ «О безопасности»
- **Федеральный закон** от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- **Федеральный закон** от 24 мая 2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»
- **Федеральный закон** от 27 декабря 2002 № 184-ФЗ «О техническом регулировании»
- **Федеральный закон** от 27 июля 2006 года № 152-ФЗ «О персональных данных»
- **Федеральный закон** от 21 июля 1993 г. № 5485-1 «О государственной тайне»
- **Федеральный закон** от 13 июня 1996 года № 63-ФЗ «Уголовный кодекс РФ»
- **Федеральный закон** от 03 апреля 1995 № 40-ФЗ «О Федеральной службе безопасности»
- **Федеральный закон** от 28 июля 2004 года № 98-ФЗ «О коммерческой тайне»
- **Федеральный закон** от 10 июня 1993 года № 5151-1 «О сертификации продукции и услуг»
- **Федеральный закон** от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях»



- Указ Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»
- Указ Президента РФ от 30.11.1995 № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»
- Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена»
- Указ Президента РФ от 12.05.2009 № 537 «О стратегии национальной безопасности Российской Федерации до 2020 года»
- Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера.
- Доктрина информационной безопасности РФ. Утверждена указом Президентом РФ от 5.12.2016 г. № 646.
- Указ Президента РФ от 11.08.2003 № 960. "Вопросы Федеральной службы безопасности РФ»
- Указ Президента РФ от 6.10.2004 г. № 1286. «Вопросы Межведомственной комиссии по защите государственной тайны»
- Указ Президента РФ от 22.05.2015 № 260 "О некоторых вопросах информационной безопасности РФ»



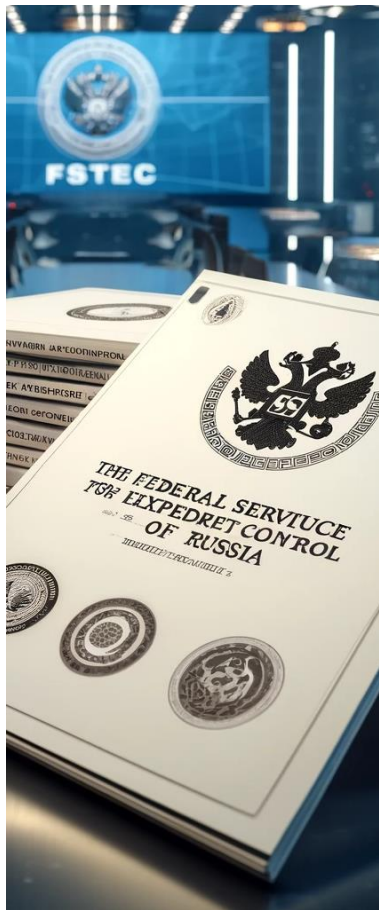
- Постановление Правительства РФ от 21.11.2011 № 957 «Об организации лицензирования отдельных видов деятельности»
- Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации»
- Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации»)
- Постановление Правительства РФ от 03.03.2012 № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»)
- Постановление Правительства РФ от 15.04.1995 № 333 «Об утверждении Положения 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»





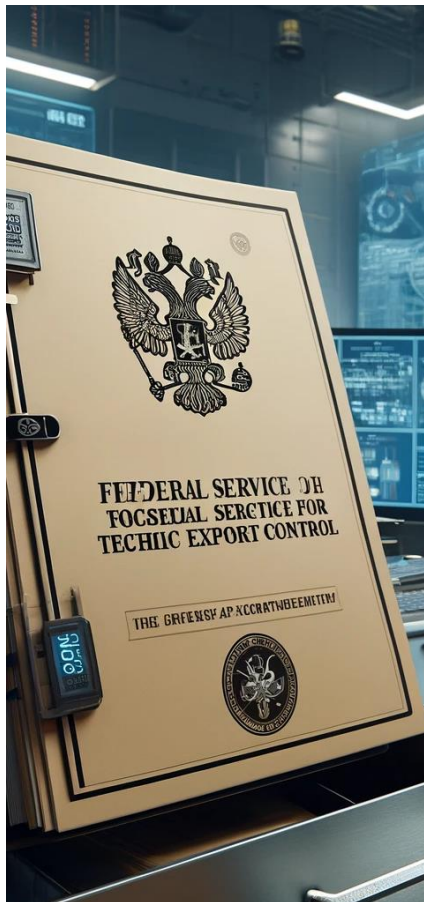
- **Постановление правительства РФ** от 16 апреля 2012 № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».
- **Постановление правительства РФ** от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом "о персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
- **Постановление правительства РФ** от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».

- **Постановление Правительства РФ** от 6 июля 2008 года № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
- **Постановление Правительства РФ** от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- **Постановление Правительства РФ** от 4 сентября 1995 г. № 870 «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».
- **Постановление Правительства РФ** от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- **Постановление Правительства РФ** от 22 ноября 2012 г. № 1205 «Об утверждении правил организации и осуществления федерального государственного контроля за обеспечением защиты государственной тайны».
- **Постановление правительства РФ** от 03.11.1994 № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
- **Постановление правительства РФ** от 16 апреля 2012 г. № 314 «Об утверждении положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».



- Положение о сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом Гостехкомиссии России от 27.10.1995 № 199.
- Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Гостехкомиссия России, 1992.
- Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации. Утверждено председателем Гостехкомиссии России 25.11.1994.
- Положение об аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Гостехкомиссии России 25.11.1994.
- Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации. Утверждено председателем Гостехкомиссии России 05.01.1996.
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30.08.2002 № 282.
- Сборник методических документов по контролю защищенности информации, обрабатываемой средствами вычислительной техники от утечки за счет побочных электромагнитных излучений и наводок. Утверждено приказом ФСТЭК России 30.12.2005 № 075.





- **Сборник временных методик оценки** защищенности конфиденциальной информации от утечки по техническим каналам. Гостехкомиссия России, 2002.
- **Руководящий документ.** Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Утверждены приказом председателя Гостехкомиссии от 19.06.2002 № 187.
- **Руководящий документ.** Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
- **Руководящий документ.** Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
- **Руководящий документ.** Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.
- **Приказ** от 18.02.2013 № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн».
- **Приказ** от 11.02.2013 № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».



- **Приказ ФСТЭК** от 20.03.2012 № 28 «Об утверждении требований к средствам антивирусной защиты» - Профили средств антивирусной защиты.
- **Приказ ФСТЭК** от 06.12.2011 № 638 «Об утверждении требований к системам обнаружения вторжений» – Профили систем обнаружения вторжений (атак).
- **Приказ ФСТЭК** от 27.09.2013 № 119 «Об утверждении требований к средствам доверенной загрузки» - Профили средств доверенной загрузки.
- **Методический документ ФСТЭК** 2014 «Рекомендации по обновлению сертифицированных средств защиты информации».
- **Приказ ФСТЭК** от 28.07.2014 № 87 «Об утверждении требований к средствам контроля съёмных носителей информации» – профили средств контроля съёмных носителей информации.
- **Методический документ ФСТЭК** 2014 «Меры защиты информации в государственных информационных системах».
- **Сообщения** «О Применении сертифицированной по требованиям БИ ОС WINDOWS XP в условиях прекращения её поддержки разработчиком», «О Применении сертифицированных по требованиям БИ ОС WINDOWS SERVER 2003 и WINDOWS SERVER 2003 R2 в условиях прекращения их поддержки разработчиком».
- **Приказ ФСТЭК** от 9.02.2016 № 9 «Об утверждении требований к межсетевым экранам» - профили средств межсетевого экранирования.



- **Приказ ФСТЭК России** от 9 августа 2018 г. № 138. «О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31, и в, «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239.
- **Приказ ФСТЭК России** от 25 декабря 2017 г. № 239. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
- **Приказ ФСТЭК России** от 22 декабря 2017 г. № 236. «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

- **Приказ ФСТЭК России** от 21 декабря 2017 г. № 235. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».
- **Приказ ФСТЭК России** от 11 декабря 2017 г. № 229. «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
- **Приказ ФСТЭК России** от 6 декабря 2017 г. № 227. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации».
- **Приказ ФСТЭК России** от 23 марта 2017 г. № 49., «О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21, и в «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31.







- **Приказ ФСТЭК России** от 15 февраля 2017 г. N 27. «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17.
- **Приказ ФСТЭК России** от 14 октября 2016 г. N 148. «Об утверждении перечня правовых актов и их отдельных частей (положений), содержащих обязательные требования, соблюдение которых оценивается ФСТЭК России при проведении мероприятий по лицензионному контролю за деятельностью по разработке и производству средств защиты конфиденциальной информации».
- **Приказ ФСТЭК России** от 14 октября 2016 г. N 147. «Об утверждении перечня правовых актов и их отдельных частей (положений), содержащих обязательные требования», соблюдение которых оценивается ФСТЭК России при проведении мероприятий по лицензионному контролю за деятельностью по технической защите конфиденциальной информации.
- **Приказ ФСТЭК России** от 14 марта 2014 г. N 31. «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Настоящие стандарты не могут быть полностью или частично воспроизведены, тиражированы и распространены в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии.

Обозначение	Наименование на русском языке
ГОСТ Р 50739-95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
ГОСТ Р 50922-2006	Защита информации. Основные требования и определения.
ГОСТ Р 51188-98	Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.
ГОСТ Р 51275-2006	Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
ГОСТ Р 51583-2014	Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
ГОСТ Р 52069.0-2013	Защита информации. Система стандартов. Основные положения.
ГОСТ Р 52447-2005	Защита информации. Техника защиты информации. Номенклатура показателей качества.
ГОСТ Р 52448-2005	Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.
ГОСТ Р 52633.0-2006	Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.

Обозначение	Наименование на русском языке
ГОСТ Р 52633.1-2009	Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных — для тестирования средств высоконадежной биометрической аутентификации.
ГОСТ Р 52633.2-2010	Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации.
ГОСТ Р 52633.3-2011	Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора.
ГОСТ Р 52633.4-2011	Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия - код доступа
ГОСТ Р 52633.5-2011	Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа.
ГОСТ Р 52633.6-2011	Защита информации. Техника защиты информации. Требования к индикации близости предъявленных биометрических данных образу «Свой».



Обозначение	Наименование на русском языке
ГОСТ Р 52863-2007	Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования.
ГОСТ Р 53109-2008	Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности.
ГОСТ Р 53110-2008	Система обеспечения информационной безопасности сети связи общего пользования. Общие положения.
ГОСТ Р 53111-2008	Устойчивость функционирования сети связи общего пользования. Требования и методы проверки.
ГОСТ Р 53112-2008	Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний.
ГОСТ Р 53113-2008	Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

Обозначение	Наименование на русском языке
ГОСТ Р 52113.2-2009	Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.
ГОСТ Р 53114-2008	Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.
ГОСТ Р 53115-2008	Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства.
ГОСТ Р 53131-2008	Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства.
ГОСТ Р 54581-2011 / ISO/IEC TR 15443-1:2005	Информационная технология Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы.
ГОСТ Р 54582-2011 / ISO/IEC TR 15443-2:2005	Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия.
ГОСТ Р 54583-2011 / ISO/IEC TR 15443-3:2007	Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3 Анализ методов доверия.

Обозначение	Наименование на русском языке
ГОСТ Р 56045-2014	Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью.
ГОСТ Р 56093-2014	Защита информации. Автоматизированные системы в защищенном исполнении. Средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования.
ГОСТ Р 56103-2014	Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения.
ГОСТ Р 56115-2014	Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования.
ГОСТ Р ИСО/МЭК 13335-1-2006	Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

Обозначение	Наименование на русском языке
ГОСТ Р ИСО 7498-1-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.
ГОСТ Р ИСО 7498-2-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.
ГОСТ Р ИСО/МЭК ТО 13335-5-2006	Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети.
ГОСТ Р ИСО/МЭК 15408-1-2012	Информационная технология Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
ГОСТ Р ИСО/МЭК 15408-2-2013	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.
ГОСТ Р ИСО/МЭК 15408-3-2013	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.
ГОСТ Р ИСО/МЭК ТО 15446-2008	Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности.
ГОСТ Р ИСО/МЭК ТО 18044-2007	Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

Обозначение	Наименование на русском языке
<b>ГОСТ Р ИСО/МЭК 18045-2013</b>	Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.
<b>ГОСТ Р ИСО/МЭК ТО 19791-2008</b>	Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.
<b>ГОСТ Р ИСО/МЭК 21827-2010</b>	Информационная технология Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса.
<b>ГОСТ Р ИСО/МЭК ТО 27000-2012</b>	Информационная технология Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.
<b>ГОСТ Р ИСО/МЭК ТО 27001-2006</b>	Информационная технология Методы и средства обеспечения безопасности. Системы — менеджмента информационной безопасности. Требования.



Обозначение	Наименование на русском языке
ГОСТ Р ИСО/МЭК 27034-1-2014	Информационная технология Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия.
ГОСТ Р ИСО/МЭК 27037-2014	Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме.
ГОСТ Р ИСО/МЭК 29100-2013	Информационная технология. Методы и средства обеспечения безопасности. Основы — обеспечения приватности.
Рекомендации по стандартизации Р 50.1.050-2004	Защита информации. Система обеспечения качества техники защиты информации. Общие положения.
Рекомендации по стандартизации Р 50.1.053-2005	Информационные технологии. Основные термины и определения в области технической защиты информации.
Рекомендации по стандартизации Р 50.1.056-2005	Техническая защита информации. Основные термины и определения.

- **BS 7799-1:2005** — Британский стандарт BS 7799 первая часть. BS 7799 Part 1 — Code of Practice for Information Security Management (Практические правила управления информационной безопасностью) описывает 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации, определённых на основе лучших примеров мирового опыта (best practices) в данной области. Этот документ служит практическим руководством по созданию СУИБ.
- **BS 7799-2:2005** — Британский стандарт BS 7799 вторая часть. BS 7799 Part 2 — Information Security management — specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию СУИБ. Вторая часть стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.
- **BS 7799-3:2006** — Британский стандарт BS 7799 третья часть. Новый стандарт в области управления рисками информационной безопасности.
- **ISO/IEC 17799:2005** — «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Международный стандарт, базирующийся на BS 7799-1:2005.
- **ISO/IEC 27000** — Словарь и определения.
- **ISO/IEC 27001** — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования». Международный стандарт, базирующийся на BS 7799-2:2005.
- **ISO/IEC 27002** — Сейчас: ISO/IEC 17799:2005. «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Дата выхода — 2007 год.
- **ISO/IEC 27005** — Сейчас: BS 7799-3:2006 — Руководство по менеджменту рисков ИБ. German Information Security Agency. IT Baseline Protection Manual — Standard security safeguards (Руководство по базовому уровню защиты информационных технологий).





- **Методический документ.** Утверждены ФСТЭК России 1 декабря 2014 г. Профили защиты средств контроля съемных машинных носителей информации.
- **Методический документ.** Утвержден ФСТЭК России 11 февраля 2014 г. Меры защиты информации в государственных информационных системах.
- **Методические документы.** Утверждены ФСТЭК России 30 декабря 2013 г. Профили защиты средств доверенной загрузки.
- **Методические документы.** Утверждены ФСТЭК России 14 июня 2012 г. Профили защиты средств антивирусной защиты.
- **Методические документы.** Утверждены ФСТЭК России 6 марта 2012 г. Профили защиты систем обнаружения вторжений.
- **Методические документы.** Утверждены ФСТЭК России 3 февраля 2012 г. Профили защиты систем обнаружения вторжений.
- **Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.** ФСТЭК России, 2008 год. Пометка «для служебного пользования» снята Решением ФСТЭК России от 16 ноября 2009 г.



- **Руководящий документ.** Гостехкомиссия России, 2003 год. Руководство по разработке профилей защиты и заданий по безопасности.
- **Руководящий документ.** Гостехкомиссия России, 2003 год. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты.
- **Руководящий документ.** Гостехкомиссия России, 2003 год. Безопасность информационных технологий. Руководство по регистрации профилей защиты.
- **Руководящий документ.** Гостехкомиссия России, 2003 год. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности.
- **Руководящий документ.** Приказ председателя Гостехкомиссии России от 19 июня 2002 г. N 187. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий.
- **Руководящий документ.** Приказ председателя Гостехкомиссии России от 4 июня 1999 г. N 114. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей.

- **Руководящий документ.** Решение председателя Гостехкомиссии России от 25 июля 1997 г. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации.
- **Руководящий документ.** Решение председателя Гостехкомиссии России от 25 июля 1997 г. Защита информации. Специальные защитные знаки. Классификация и общие требования.
- **Руководящий документ.** Решение председателя Гостехкомиссии России от 30 марта 1992 г. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
- **Руководящий документ.** Решение председателя Гостехкомиссии России от 30 марта 1992 г. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
- **Руководящий документ.** Решение председателя Гостехкомиссии России от 30 марта 1992 г. Защита от несанкционированного доступа к информации. Термины и определения.
- **Руководящий документ.** Решение председателя Гостехкомиссии России от 30 марта 1992 г. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
- **Руководящий документ.** Решение председателя Гостехкомиссии России от 30 марта 1992 г. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.

Постановление Правительства от 16.04.2012 № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».







Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

**Приказ ФАПСИ при Президенте России от  
13.06.2001 г. № 152**

**Зарегистрирован в Минюсте РО 6 августа 2001 г.  
№ 2848**

Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

**Приказ ФСБ России от 09.02.2005 г. № 66  
Зарегистрирован в Минюсте РФ 3 марта 2005 г.  
№ 6382**



Методические рекомендации по обеспечению с помощью криптографических средств безопасности персональных данных при их обработке в ИСПДн с использованием средств автоматизации.

**Приказ ФСБ России от 21 февраля 2008 г.  
№ 149/54-144**

Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в ИСПДн.

**Приказ ФСБ России от 21 февраля 2008 г.  
№ 149/6/6-622**





Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством российской федерации требований к защите персональных данных для каждого из уровней защищенности

*Приказ ФСБ России от 10 июля 2014 г. № 378*

**Приказ ФСБ России от 21 февраля 2008 г.  
№ 149/6/6-622**

## Основные нормативные правовые акты в области защиты коммерческой тайны и иной конфиденциальной информации



- **Федеральный закон** от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- **Федеральный закон** от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».
- **Федеральный закон** от 7 июля 2003 г. № 126-ФЗ «О связи».
- **Федеральный закон** от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
- **Федеральный закон** от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».
- **Федеральный закон** от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
- **Федеральный закон** от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности».





- **Указ Президента Российской Федерации** от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
- **Указ Президента Российской Федерации** от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации».
- **Указ Президента Российской Федерации** от 17.03.2008 г. №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
- **Указ Президента Российской Федерации** от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
- **Постановление Правительства Российской Федерации** от 3 ноября 1994 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».



## Акты Правительства РФ

Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утверждено постановлением Совета Министров - Правительства Российской Федерации от 15 сентября 1993 г. № 912-51

## Ведомственные акты

Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 г. N 282

Спасибо за внимание!

Вопросы?