# Нормативная база обеспечения защиты информации

**Учебные вопросы:**

1. Международная нормативная база обеспечения безопасности.

2. Федеральная нормативная база обеспечения безопасности.

3. Руководящие документы и методические указания в сфере защиты информации

4. Совершенствование нормативной базы защиты информации.

## Международная нормативная база обеспечения безопасности.

За рубежом разработка стандартов проводится непрерывно, последовательно публикуются проекты и версии стандартов на разных стадиях согласования и утверждения. Некоторые стандарты поэтапно углубляются и детализируются в виде совокупности взаимосвязанных по концепциям и структуре групп стандартов.

Принято считать, что неотъемлемой частью общего процесса стандартизации информационных технологий (ИТ) является разработка стандартов, связанных с проблемой безопасности ИТ, которая приобрела большую актуальность в связи с тенденциями все большей взаимной интеграции прикладных задач, построения их на базе распределенной обработки данных, систем телекоммуникаций, технологий обмена электронными данными.

Разработка стандартов для открытых систем, в том числе и стандартов в области безопасности ИТ, осуществляется рядом специализированных международных организаций и консорциумов таких, как, например, ISO, IЕС, ITU-T, IEEE, IАВ, WOS, ЕСМА, X/Open, OSF, OMG и др.

Значительная работа по стандартизации вопросов безопасности ИТ проводится специализированными организациями и на национальном уровне. Все это позволило к настоящему времени сформировать достаточно обширную методическую базу, в виде международных, национальных и отраслевых стандартов, а также нормативных и руководящих материалов, регламентирующих деятельность в области безопасности ИТ.

***Архитектура безопасности Взаимосвязи открытых систем***

Большинство современных сложных сетевых структур, лежащих в качестве телекоммуникационной основы существующих АС проектируются с учетом идеологии Эталонной модели (ЭМ) Взаимосвязи открытых систем (ВОС), которая позволяет оконечному пользователю сети (или его прикладным процессам) получить доступ к информационно-вычислительным ресурсам значительно легче, чем это было раньше. Вместе с тем концепция открытости систем создает ряд трудностей в организации защиты информации в ВС. Требование защиты ресурсов сети от НСД является обязательным при проектировании и реализации большинства современных ИВС, соответствующих ЭМ ВОС.

В 1986 г. рядом международных организаций была принята Архитектура безопасности ВОС (АБ ВОС). В архитектуре ВОС выделяют семь уровней иерархии: физический, канальный, сетевой, транспортный, сеансовый, представительный и прикладной. Однако в АБ ВОС предусмотрена реализация механизмов защиты в основном на пяти уровнях. Для защиты информации на физическом и канальном уровне обычно вводится такой механизм защиты, как линейное шифрование. Канальное шифрование обеспечивает закрытие физических каналов связи с помощью специальных шифраторов. Однако применение только канального шифрования не обеспечивает полного закрытия информации при ее передаче по ИВС, так как на узлах коммутации пакетов информация будет находиться в открытом виде. Поэтому НСД нарушителя к аппаратуре одного узла ведет к раскрытию всего потока сообщений, проходящих через этот узел. В том случае, когда устанавливается виртуальное соединение между двумя абонентами сети и коммуникации, в данном случае, проходят по незащищенным элементам ИВС, необходимо сквозное шифрование, когда закрывается информационная часть сообщения, а заголовки сообщений не шифруются. Это позволяет свободно управлять потоками зашифрованных сообщений. Сквозное шифрование организуется на сетевом и/или транспортном уровнях согласно ЭМ ВОС. На прикладном уровне реализуется большинство механизмов защиты, необходимых для полного решения проблем обеспечения безопасности данных в ИВС.

АБ ВОС устанавливает следующие службы безопасности:

* обеспечения целостности данных (с установлением соединения, без установления соединения и для выборочных полей сообщений);
* обеспечения конфиденциальности данных (с установлением соединения, без установления соединения и для выборочных полей сообщений);
* контроля доступа;
* аутентификации (одноуровневых объектов и источника данных);
* обеспечения конфиденциальности трафика;
* обеспечения невозможности отказа от факта отправки сообщения абонентом - передатчиком и приема сообщения абонентом - приемником.

***Состояние международной нормативно-методической базы***

С целью систематизации анализа текущего состояния международной нормативно-методической базы в области безопасности ИТ необходимо использовать некоторую классификацию направлений стандартизации. В общем случае, можно выделить следующие направления.

1. Общие принципы управления информационной безопасностью.
2. Модели безопасности ИТ.
3. Методы и механизмы безопасности ИТ (такие, как, например: методы аутентификации, управления ключами и т.п.).
4. Криптографические алгоритмы.
5. Методы оценки безопасности информационных систем.
6. Безопасность EDI-технологий.
7. Безопасность межсетевых взаимодействий (межсетевые экраны).
8. Сертификация и аттестация объектов стандартизации.

***Стандартизация вопросов управления информационной безопасностью***

Анализ проблемы защиты информации в информационных системах требует, как правило, комплексного подхода, использующего общеметодологические концептуальные решения, которые позволяют определить необходимый системообразующей контекст для редуцирования общей задачи управления безопасностью ИТ к решению частных задач. Поэтому в настоящее время возрастает роль стандартов и регламентирующих материалов общеметодологического назначения.

На роль такого документа претендует, находящийся в стадии утверждения проект международного стандарта ISO/IEC DTR 13335-1,2,3 - "Информационная технология. Руководство по управлению безопасностью информационных технологий". Данный документ содержит:

* определения важнейших понятий, непосредственно связанных с проблемой управления безопасностью ИТ; - определение важных архитектурных решений по созданию систем управления безопасностью ИТ (СУБ ИТ), в том числе, определение состава элементов, задач, механизмов и методов СУБ ИТ;
* описание типового жизненного цикла и принципов функционирования СУБ ИТ;
* описание принципов формирования политики (методики) управления безопасностью ИТ;
* методику анализа исходных данных для построения СУБ ИТ, в частности методику идентификации и анализа состава объектов защиты, уязвимых мест информационной системы, угроз безопасности и рисков и др.;
* методику выбора соответствующих мер защиты и оценки остаточного риска;
* принципы построения организационного обеспечения управления в СУБ ИТ и пр.

***Стандартизация моделей безопасности ИТ***

С целью обеспечения большей обоснованности программно-технических решений при построении СУБ ИТ, а также определения ее степени гарантированности, необходимо использование возможно более точных описательных моделей как на общесистемном (архитектурном) уровне, так и на уровне отдельных аспектов и средств СУБ ИТ.

Построение моделей позволяет структурировать и конкретизировать исследуемые объекты, устранить неоднозначности в их понимании, разбить решаемую задачу на подзадачи, и, в конечном итоге, выработать необходимые решения.

Можно выделить следующие международные стандарты и другие документы, в которых определяются основные модели безопасности ИТ:

* ISO/IEC 7498-2-89 - "Информационные технологии. Взаимосвязь открытых системы. Базовая эталонная модель. Часть 2. Архитектура информационной безопасности";
* ISO/IEC DTR 10181-1 - "Информационные технологии. Взаимосвязь открытых систем. Основы защиты информации для открытых систем. Часть 1. Общее описание основ защиты информации ВОС";
* ISO/IEC DTR 10745 - "Информационные технологии. Взаимосвязь открытых систем. Модель защиты информации верхних уровней";
* ISO/IEC DTR 11586-1 - "Информационные технологии. Взаимосвязь открытых систем. Общие функции защиты верхних уровней. Часть 1. Общее описание, модели и нотация";
* ISO/IEC DTR 13335-1 - "Информационные технологии. Руководство по управлению безопасностью информационных технологий. Часть 1. Концепции и модели безопасности информационных технологий".<

***Стандартизация методов и механизмов безопасности ИТ***

На определенном этапе задача защиты информационных технологий разбивается на частные подзадачи, такие как обеспечение, конфиденциальности, целостности и доступности. Для этих подзадач должны вырабатываться конкретные решения по организации взаимодействия объектов и субъектов информационных систем. К таким решениям относятся методы:

* аутентификации субъектов и объектов информационного взаимодействия, предназначенные для предоставления взаимодействующим сторонам возможности удостовериться, что противоположная сторона действительно является тем, за кого себя выдает;
* шифрования информации, предназначенные для защиты информации в случае перехвата ее третьими лицами;
* контроля целостности, предназначенные для обеспечения того, чтобы информация не была искажена или подменена;
* управления доступом, предназначенные для разграничения доступа к информации различных пользователей; - повышения надежности и отказоустойчивости функционирования системы, предназначенные для обеспечения гарантий выполнения информационной системой целевых функций;
* управления ключами, предназначенные для организации создания, распространения и использования ключей субъектов и объектов информационной системы, с целью создания необходимого базиса для процедур аутентификации, шифрования, контроля подлинности и управления доступом.

Организации по стандартизации уделяют большое внимание разработке типовых решений для указанных выше аспектов безопасности. К ним, в первую очередь отнесем следующие международные стандарты:

* ISO/IEC 9798-91 - "Информационные технологии. Защита информации. Аутентификация объекта".

Часть 1. Модель.

Часть 2. Механизмы, использующие симметричные криптографические алгоритмы.

Часть 3. Аутентификация на базе алгоритмов с открытыми ключами.

Часть 4. Механизмы, использующие криптографическую контрольную функцию.

Часть 5. Механизмы, использующие алгоритмы с нулевым разглашением.

* ISO/IEC 09594-8-88 - "Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации";
* ISO/IEC 11577-94 - "Информационные технологии. Передача данных и обмен информацией между системами. Взаимосвязь открытых систем. Протокол защиты информации на сетевом уровне";
* ISO/IEC DTR 10736 - "Информационные технологии. Передача данных и обмен информацией между системами. Протокол защиты информации на транспортном уровне";
* ISO/IEC CD 13888 - "Механизмы предотвращения отрицания".

Часть 1. Общая модель.  
Часть 2. Использование симметричных методов.  
Часть 3. Использование асимметричных методов;

* ISO/IEC 8732-88 - "Банковское дело. Управление ключами";
* ISO/IEC 11568-94 - "Банковское дело. Управление ключами".

Часть 1. Введение. Управление ключами.  
Часть 2. Методы управления ключами для симметричных шифров.  
Часть 3. Жизненный цикл ключа для симметричных шифров;

* ISO/IEC 11166-94 - "Банковское дело. Управление ключами посредством асимметричного алгоритма".

Часть 1. Принципы процедуры и форматы.  
Часть 2. Принятые алгоритмы, использующие криптосистему RSA;

* ISO/IEC DIS 13492 - "Банковское дело. Управление ключами, относящимися к элементам данных";
* ISO/IEC CD 11770 - "Информационные технологии. Защита информации. Управление ключами".

Часть 1. Общие положения.  
Часть 2. Механизмы, использующие симметричные методы.  
Часть 3. Механизмы, использующие асимметричные методы;

* ISO/IEC DTR 10181- "Информационные технологии. Взаимосвязь открытых систем. Основы защиты информации для открытых систем".

Часть 1. Общее описание основ защиты информации в ВОС.  
Часть 2. Основы аутентификации.  
Часть 3. Управление доступом.  
Часть 4. Безотказность получения.  
Часть 5. Конфиденциальность.  
Часть 6. Целостность.  
Часть 7. Основы проверки защиты.

К этому же уровню следует отнести стандарты, описывающие интерфейсы механизмов безопасности ИТ:

* ISO/IEC 10164-7-92. "Информационные технологии. Взаимосвязь открытых систем. Административное управление системы. Часть 7. Функции уведомления о нарушениях информационной безопасности".
* ISO/IEC DTR 11586. "Информационные технологии. Взаимосвязь открытых систем. Общие функции защиты верхних уровней".

Часть 1. Общее описание, модели и нотация.

Часть 2. Определение услуг сервисного элемента обмена информацией защиты.

Часть 3. Спецификация протокола сервисного элемента обмена информацией защиты.

Часть 4. Спецификация синтаксиса защищенной передачи.

В стандартах этого уровня, как правило, не указываются конкретные криптографические алгоритмы, а декларируется, что может быть использован любой криптоалгоритм, при этом подразумевалось использование определенных зарубежных криптографических алгоритмов. Поэтому в ряде случаев при использовании некоторых стандартов может потребоваться их адаптация к отечественным криптоалгоритмам.

***Стандартизация международных криптографических алгоритмов***

ISO стандартизировала ряд криптографических алгоритмов в таких международных стандартах, как, например:

* ISO/IEC 10126-2-91 - "Банковское дело. Процедуры шифрования сообщения. Часть 2. Алгоритм DEA";
* ISO/IEC 8732-87 - "Информационные технологии. Защита информации. Режимы использования 64-битного блочного алгоритма";
* ISO/IEC 10116-91- "Банковское дело. Режимы работы n-бит блочного алгоритма шифрования";
* ISO/IEC 10118-1,2-88 - "Информационные технологии. Шифрование данных. Хэш-функция для цифровой подписи";
* ISO/IEC CD 10118-3,4 - "Информационные технологии. Защита информации. Функции хэширования";
* ISO/IEC 9796-91 - "Информационные технологии. Схема электронной подписи, при которой производится восстановление сообщения";
* ISO/IEC CD 14888 - "Информационные технологии. Защита информации. Цифровая подпись с добавлением". Однако широкое внедрение этих алгоритмов представляется малореальным, поскольку политика крупных государств направлена, как правило, на использование собственных криптоалгоритмов.

## Федеральная нормативная база обеспечения безопасности.

**Основные нормативно-правовые акты и методические документы в области защиты информации**

 1. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

2. Стратегия развития информационного общества в Российской Федерации, утверждённая Президентом Российской Федерации 07.02.2008 № Пр-212.

3. Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденная  Указом Президента Российской Федерации от 12 мая 2009 г. № 537.

4\*. Основы организации защиты информации в Приволжском федеральном округе (Одобрены  Решением Координационного Совета по защите информации при полномочном представителе Президента Российской Федерации в Приволжском федеральном округе от 12 ноября 2009 года).

**Основные общие нормативные правовые акты**

1. Конституция Российской Федерации.

2. Федеральный [закон Российской Федерации от 28 декабря 2010 г. № 390-ФЗ «О безопасности»](http://www.fstec.ru/_docs/doc_1_2_002.htm)

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации»

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»

5. «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 15.09.1993 г. № 912-51.

**По вопросам защиты информации ограниченного доступа, не содержащей сведения государственной тайны (конфиденциальность информации, доступ к которой ограничен федеральными законами)**

1. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».

2. 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».

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

4. Указ Президента Российской Федерации от 17.03.2008 № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена".

5. Приказ Федеральной службы охраны Российской Федерации от 7.08.2009 № 487 "Об утверждении положения о сегменте информационно-телекоммуникационной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

6. Приказ ФСТЭК России от 28 августа 2007 г. № 181 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по технической защите конфиденциальной информации».

7. Приказ ФСТЭК России от 28 августа 2007 г. № 182 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

**По вопросам безопасности информационных систем персональных данных**

1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2. Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных".

3. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

4. Постановление Правительства РФ от 6 июля 2008 г. N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных".

5. \*  Постановление Правительства Российской Федерации от 15 мая 2010 г. № 330 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством РФ информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскании), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг)».

6. Постановление Правительства РФ от 21.03.2012 N 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".

7. Порядок проведения классификации информационных систем персональных данных. Утвержден приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.

9. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных".  Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.

10. Приказ ФСТЭК  России от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных».

11. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации" от 21 февраля 2008 года № 149/54-144.

12. 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 информационных системах персональных данных" от 21 февраля 2008 года № 149/6/6-622.

13. Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

14. Административный регламент исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных. Утвержден приказом Минкомсвязи от 14.11.2011 г. № 312.

15. Приказ Министерства связи и массовых коммуникаций РФ от 30 января 2010г. N18 "Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции "Ведение реестра операторов, осуществляющих обработку персональных данных".

16. Приказ Роскомнадзора от 19 августа 2011 г. № 706 "Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных".

**По вопросам безопасности информационных систем общего пользования**

1. Постановление Правительства Российской Федерации от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».

2. Приказ Министерства связи и массовых коммуникаций РФ от 25 августа 2009 г. N 104 "Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования"

3. Приказ ФСБ РФ и ФСТЭК РФ от 31.08.2010 № 416/489 "Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования"

4. Приказ Министерства экономического развития Российской Федерации от 16.11.2009 № 470 "О требованиях к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами федеральных органов исполнительной власти".

5. Постановление Правительства Самарской области от 13.08.2010 № 380 "Об обеспечении доступа к информации о деятельности Правительства Самарской области и органов исполнительной власти Самарской области, размещаемой в сети интернет.

**По вопросам электронной цифровой подписи**

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

2. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

3. Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

**Сопутствующие нормативные правовые акты по безопасности информации**

1. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

2. Федеральный закон РФ от 29 июля 2004 г № 98-ФЗ «О коммерческой тайне».

3. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

4. Постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности»

5. Постановление Правительства Российской Федерации от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».

**Организационно – распорядительные документы**

**Положения**

1. Положение о Федеральной службе по техническому и экспортному контролю, Утверждено Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

2. Положение о государственном лицензировании деятельности в  области защиты информации, Решение Гостехкомиссии России и ФАПСИ от 27 апреля 1994 г. № 10.

3. Положение о лицензировании деятельности по технической защите конфиденциальной информации, Утверждено постановлением Правительства Российской Федерации от 03 февраля 2012 г. № 79. [ПП РФ 03.02.2012 О лицензировании ТЗКИ.doc](http://dit.samregion.ru/external/ministry/files/c_1815/PP_RF_03.02.2012_O_litsenzirovanii_TZKI.doc).

4. Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации, Утверждено постановлением Правительства Российской Федерации от 3 марта 2012 г. N 171.

5. Положение 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), Утверждено постановлением Правительства Российской Федерации от 16.04.2012 N 313.

6. Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 31 августа 2006 г. № 532.

7. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации  от 26 июня 1995 г. № 608.

8. Положение о сертификации средств защиты информации по требованиям безопасности информации, утвержденное приказом Гостехкомиссии России от 27 октября 1995 г. № 199.

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

10. Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.

11. Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом председателя Гостехкомиссии России  от 5 января 1996 г. № 3.

12. Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации. Утверждено приказом председателя Гостехкомиссии России от 5 января 1996 г. № 3.

13. Типовое положение об испытательной лаборатории, утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.

14. Типовое положение о Совете (Технической комиссии) министерства, ведомства, органа государственной власти субъекта Российской Федерации по защите информации от иностранных технических разведок и от ее утечки по техническим каналам. Решение Гостехкомиссии при Президенте Российской Федерации от 14.03.1995 г. № 32.

15. Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в министерствах и ведомствах, в органах государственной власти субъектов Российской Федерации.  Решение Гостехкомиссии при Президенте Российской Федерации от 14.03.1995 № 32.

16. Правила предоставления документов по вопросам лицензирования в форме электронных документов, Утверждены постановлением Правительства Российской Федерации от 16 июля 2012 г. № 722.

## Руководящие документы и методические указания в сфере защиты информации

**Специальные нормативные документы**

Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, Решение председателя Гостехкомиссии России от 30 марта 1992 г.

Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения, Решение председателя Гостехкомиссии России от 30 марта 1992 г.

Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации, Решение председателя Гостехкомиссии России от 30 марта 1992 г.

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации, Решение председателя Гостехкомиссии России от 30 марта 1992 г.

Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники, Решение председателя Гостехкомиссии России от 30 марта 1992 г.

Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации Решение председателя Гостехкомиссии России от 25 июля 1997 г.

Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования Решение председателя Гостехкомиссии России от 25 июля 1997 г.

Руководящий документ. 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.

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Утвержден приказом Гостехкомиссии России от 19 июня 2002 г. № 187 ([часть 1](http://www.fstec.ru/_docs/ch%201.doc), [часть 2](http://www.fstec.ru/_docs/ch%202.doc), [часть 3](http://www.fstec.ru/_docs/ch%203.doc)).

Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности, Гостехкомиссия России, 2003 год.

Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты, Гостехкомиссия России, 2003 год.

Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты, Гостехкомиссия России, 2003 год.

Руководство по разработке профилей защиты и заданий по безопасности, Гостехкомиссия России, 2003 год.

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).*

Методический документ ФСТЭК России ИТ.СОВ.С4.ПЗ "Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты".

Методический документ ФСТЭК России ИТ.СОВ.С5.ПЗ "Профиль защиты систем обнаружения вторжений уровня сети пятого класса защиты".

Методический документ ФСТЭК России ИТ.СОВ.С6.ПЗ "Профиль защиты систем обнаружения вторжений уровня сети шестого класса защиты".

Методический документ ФСТЭК России ИТ.СОВ.У4.ПЗ "Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты".

Методический документ ФСТЭК России ИТ.СОВ.У5.ПЗ "Профиль защиты систем обнаружения вторжений уровня узла пятого класса защиты".

Методический документ ФСТЭК России ИТ.СОВ.У6.ПЗ "Профиль защиты систем обнаружения вторжений уровня узла шестого класса защиты".

Методический документ ФСТЭК России. Профиль защиты средств антивирусной защиты типа "А" четвертого класса защиты.

Методический документ ФСТЭК России. Профиль защиты средств антивирусной защиты типа "А" пятого класса защиты.

Методический документ ФСТЭК России. Профиль защиты средств антивирусной защиты типа "А" шестого класса защиты.

Методический документ ФСТЭК России. Профиль защиты средств антивирусной защиты типа "Б" четвертого класса защиты.

Методический документ ФСТЭК России. Профиль защиты средств антивирусной защиты типа "Б" пятого класса защиты.

Методический документ ФСТЭК России. Профиль защиты средств антивирусной защиты типа "Б" шестого класса защиты.

Методический документ ФСТЭК России. Профиль защиты средств антивирусной защиты типа "В" четвертого класса защиты.

Методический документ ФСТЭК России. Профиль защиты средств антивирусной защиты типа "В" пятого класса защиты.

Методический документ ФСТЭК России. Профиль защиты средств антивирусной защиты типа "В" шестого класса защиты.

Методический документ ФСТЭК России. Профиль защиты средств антивирусной защиты типа "Г" четвертого класса защиты.

Методический документ ФСТЭК России. Профиль защиты средств антивирусной защиты типа "Г" пятого класса защиты.

Методический документ ФСТЭК России. Профиль защиты средств антивирусной защиты типа "Г" шестого класса защиты.

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

«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.\**

«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.*

*\* - Документ ограниченного распространения*

**Информационные письма (сообщения)**

1.Информационное сообщение ФСТЭК России N 240/24/1701 от 04.05.2012 "О работах в области оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа"

2. Информационное сообщение ФСТЭК России N 240/22/2222 от 30.05.2012 "По вопросу необходимости получения лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации"

3. Информационное письмо ФСТЭК России № 240 от 01.03.2012 "Об утверждении требований к системам обнаружения вторжений".

4. Информационное сообщение ФСТЭК России N 240/24/3095 от 30.07.2012 "Об утверждении Требований к средствам антивирусной защиты".

**По вопросам безопасности информации в ключевых системах информационных инфраструктурах**

1.\* Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий. Утверждена Секретарем Совета Безопасности Российской Федерации 8 ноября 2005 г.

2.\* Положение о реестре ключевых систем информационной инфраструктуры. Утверждено приказом ФСТЭК России от 4 марта 2009 г. №74.

Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры. Утверждены заместителем директора ФСТЭК России 19 ноября 2007 года.

3. \* Методика определения актуальных угроз безопасности информации в КСИИ. Утверждена заместителем директора ФСТЭК России 18 мая 2007 года

4. \* Базовая модель угроз безопасности информации в КСИИ. Утверждена заместителем директора ФСТЭК России 18 мая 2007 года.

5. \* Общие требования по обеспечению безопасности информации в КСИИ. Утверждены заместителем директора ФСТЭК России 18 мая 2007 года.

6. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации.

**Государственные стандарты**

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

2. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Госстандарт России.

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

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

5. ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России.

6. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Госстандарт России.

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

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

9. ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России.

10. ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России.

11. ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России.

## Совершенствование нормативной базы защиты информации.

***Совершенствование нормативного правового обеспечения информационной безопасности Российской Федерации должно осуществляться по направлениям развития*:**

* общепризнанных принципов и норм международного права, международных договоров Российской Федерации и нормативных правовых актов международных организаций, участником которых является Российской Федерация;
* федерального законодательства, регулирующего отношения в данной области по предметам ведения Российской Федерации и совместного ведения Российской Федерации и ее субъектов;
* законодательства субъектов Российской Федерации, регулирующего отношения в рассматриваемой области по вопросам, отнесенным к предметам совместного ведения Российской Федерации и субъектов Российской Федерации, а также собственного правового регулирования субъектов Российской Федерации;
* нормативных правовых актов федеральных органов исполнительной власти, принимаемых в пределах их полномочий.

В рамках совершенствования нормативного правового обеспечения информационной безопасности Российской Федерации должны быть конкретизирован перечень объектов обеспечения безопасности и уточнены правовые механизмы регулирования отношений в области противодействия угрозам безопасности этих объектов.

**Основными целями совершенствования системы общепризнанных принципов и норм международного права, системы международных договоров Российской Федерации и нормативных правовых актов международных организаций, участником которых является Российской Федерация, являются:**

* создание комплексной системы международной информационной безопасности, предусматривающей координацию усилий всех членов мирового сообщества по противодействию наиболее опасным угрозам безопасности международной информационной сферы и информационной сферы каждой страны;
* развитие системы международных договоров по отдельным направлениям обеспечения информационной безопасности Российской Федерации.

Основными целями совершенствования федерального законодательства в области обеспечения информационной безопасности являются:

* повышение эффективности правового регулирования отношений в области противодействия угрозам национальным интересам Российской Федерации в информационной сфере;
* формирование комплексной системы согласованных нормативных правовых актов Российской Федерации, регулирующих отношения в рассматриваемой области и затрагивающих вопросы, отнесенные к ведению Российской Федерации и ее совместному ведению с субъектами Российской Федерации.

**Основными целями совершенствования законодательства субъектов Российской Федерации в области информационной безопасности являются:**

* формирование системы обеспечения информационной безопасности субъектов Российской Федерации как составной части единой системы обеспечения информационной безопасности Российской Федерации;
* согласование направлений развития региональных информационных инфраструктур, принципов и механизмов их взаимодействия с федеральной информационной инфраструктурой, сохранение и развитие единого информационного пространства Российской Федерации.

Основными целями совершенствования нормативных правовых актов федеральных органов исполнительной власти Российской Федерации в области информационной безопасности являются конкретизация правовых механизмов реализации норм международного права и национального законодательства.

Совершенствование нормативного правового обеспечения информационной безопасности Российской Федерации осуществляется на основе максимально возможного сохранения системы действующих нормативных правовых актов и основных механизмов регулирования общественных отношений в области противодействия угрозам интересам Российской Федерации в информационной сфере.

Противодействие этим угрозам предполагает создание системы эффективного взаимодействия общества и государства в целях предупреждения, выявления и пресечения правонарушений в области обеспечения информационной безопасности Российской Федерации на основе расширения участия общественных организаций в контроле за соблюдением международных договоров Российской Федерации и законодательства Российской Федерации в области защиты прав и свобод человека, установления порядка взаимодействия общественных организаций с федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации в целях обеспечения информационной безопасности России.

**Совершенствование системы общепризнанных принципов и норм международного права, системы международных договоров Российской Федерации и нормативных правовых актов международных организаций, участником которых является Российская Федерация, должно осуществляться по следующим основным направлениям:**

* закрепление права на безопасность функционирования глобальных информационно-телекоммуникационных систем и сетей связи, на сохранность передаваемой в них информации в качестве общепризнанной нормы международного права;
* создание международной системы обеспечения безопасности глобальных информационных и телекоммуникационных систем и сетей связи, включая предотвращение и разрешение конфликтных ситуаций, возникающих при использовании этих систем и сетей, защиту законных интересов человека и гражданина, связанных с безопасностью информационного обмена, охрану объектов интеллектуальной собственности, обеспечение неприкосновенности частной жизни, личной и семейной тайны, тайны сообщений в интенсивно развивающихся глобальных информационно-телекоммуникационных системах;

предотвращение создания и использования средств нарушения нормального функционирования международных и национальных информационных и телекоммуникационных систем и сетей связи, а также несанкционированного доступа к информационным ресурсам;

* присоединение к международным договорам по тарифам и услугам в области телекоммуникаций, а также по борьбе с преступлениями в сфере высоких технологий;
* присоединение к Конвенции о международном праве опровержения (1953г.) и продвижение идеи присоединения к ней других государств;
* расширение участия российских научных организаций в фундаментальных и поисковых исследованиях, проводимых международными организациями.

**Совершенствование федерального законодательства должно осуществляться по следующим направлениям:**

* усиление гарантий конституционных прав и свобод граждан, реализуемых в информационной сфере;
* развитие правовых механизмов регулирования общественных отношений в области конституционных ограничений прав и свобод человека и гражданина, реализуемые в информационной сфере, в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;
* обеспечение государственной поддержки фундаментальных, поисковых и опытно-конструкторских работ в области создания конкурентоспособных средств информатизации, телекоммуникации и связи;
* стимулирование инвестиций в производство конкурентоспособных средств информатизации, телекоммуникации и связи, их продвижение на внутренний и мировой рынки;
* развитие системы обеспечения информационной безопасности Российской Федерации, прежде всего, за счет включения в нее органов государственной власти субъектов Российской Федерации, общественных объединений, организаций и граждан;
* создание системы государственного управления информационными ресурсами;
* совершенствование законодательства, регулирующего отношения в области международного информационного обмена;
* совершенствование законодательства по вопросам защиты государственной тайны, предотвращения несанкционированного доступа к другим охраняемым законом сведениям;
* совершенствование законодательства по вопросам защиты конфиденциальной информации;
* законодательное разграничение уровней правового регулирования проблем обеспечения информационной безопасности (федеральный уровень, уровень субъекта Федерации, уровень местного самоуправления).

**Совершенствование законодательства субъектов Российской Федерации должно осуществляться по следующим направлениям:**

приведение в соответствие с федеральным законодательством по вопросам, отнесенным к совместному ведению Российской Федерации и ее субъектов;

внесение изменений и дополнений в действующее законодательство субъектов Федерации в области обеспечения информационной безопасности для устранения противоречий нормам Конституции Российской Федерации, федеральному законодательству и международным соглашениям, к которым присоединилась Российская Федерация, а также конкретизация норм ответственности за правонарушения в данной области;

согласование усилий органов государственной власти субъектов Российской Федерации и федеральных органов государственной власти по решению проблем обеспечения безопасности региональных информационных и телекоммуникационных систем и информационных ресурсов;

поддержка отечественных товаропроизводителей конкурентоспособных средств информатизации, телекоммуникации и связи, содействие в продвижении их продукции на внутренний и мировой рынки;

повышение экономической эффективности использования региональных информационных ресурсов, введения их в хозяйственный оборот.

* нормативных правовых актов федеральных органов исполнительной власти, принимаемых в пределах их полномочий.