Стандарты информационной безопасности

Лекция 1. Введение. Роль стандартов и спецификаций. Обзор стандартов и спецификаций в области информационной безопасности

Направление подготовки (специальность):

10.03.01 Информационная безопасность

Руководитель занятий:

Куприянов Александр Олегович

Количество часов:

2 часа

Роль стандартов и спецификаций

Конституционным органом, осуществляющим подготовку решений Президента Российской Федерации в области обеспечения безопасности (Закон Российской Федерации от 5 марта 1992 г. "О безопасности", раздел III) является Совет Безопасности Российской Федерации. В Конституции Российской Федерации Совет Безопасности закреплен как государственный орган в статье 83 (п. "ж"), определяющей полномочия Президента Российской Федерации в отношении формирования важнейших институтов государства (Правительство, Центральный банк, федеральные суды, Генеральный прокурор, Администрация Президента, высшее командование Вооруженных Сил Российской Федерации).

На Совет Безопасности как конституционный орган, осуществляющий подготовку решений Президента Российской Федерации в области обеспечения безопасности, возлагалось рассмотрение стратегических проблем государственной, экономической, общественной, оборонной, информационной, экологической и иных видов безопасности, охраны здоровья населения, прогнозирования, предотвращения чрезвычайных ситуаций и преодоления их последствий, обеспечения стабильности и правопорядка.

Основополагающие документы документы в области информационной безопасности

№ п/п	Перечень нормативно-правовых документов	
1	Конституция Российской Федерации (Статья 83)	
2	Федеральный закон "О безопасности"	28 декабря 2010 года № 390-ФЗ
3	Стратегия национальной безопасности Российской Федерации	Указ Президента РФ от 02.07.2021 № 400
4	Доктрина информационной безопасности Российской Федерации	Указ Президента РФ от 05.12.2016 № 646
5	Конвенция об обеспечении международной информационной безопасности (концепция)	
6	Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации	Утверждены Президентом Российской Федерации Д. Медведевым 3 февраля 2012 г., № 803
7	Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года	Указ Президента РФ от 12.04.2021 № 213
8	Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации	Утверждены Секретарем Совета Безопасности Российской Федерации 31.08.2017
9	Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации	Утверждена Президентом Российской Федерации 12.12.2014 № К 1274

Структура документов в области информационной безопасности в Российской Федерации

<table>
<tr><th colspan="3">Нормативные документы
в области информационной безопасности и защиты информации</th></tr>
<tr><td rowspan="2">Нормативно-правовые акты</td><td colspan="2">Нормативно-методические и технические документы</td></tr>
<tr><td>Методические документы федеральных органов</td><td>Стандарты информационной безопасности</td></tr>
<tr><td>Международные договоры РФ</td><td rowspan="6">Статья 5. Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании"
Требования, установленные государственными заказчиками, федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности, обороны, внешней разведки, противодействия техническим разведкам и технической защиты информации, государственного управления использованием атомной энергии, государственного регулирования безопасности при использовании атомной энергии, и (или) государственными контрактами (договорами)</td><td>Международные стандарты</td></tr>
<tr><td>Конституция РФ</td><td>Государственные (национальные) стандарты РФ</td></tr>
<tr><td>Законы федерального уровня (включая федеральные конституционные законы, кодексы)</td><td>Рекомендации по стандартизации</td></tr>
<tr><td>Указы Президента РФ</td><td>Методические указания</td></tr>
<tr><td>Постановления правительства РФ</td><td></td></tr>
<tr><td>Нормативные правовые акты федеральных министерств и ведомств</td><td></td></tr>
<tr><td>Нормативные правовые акты субъектов РФ, органов местного самоуправления</td><td></td></tr>
</table>

Основные законы об информационной безопасности в РФ

№ п/п	Перечень нормативно-правовых документов	Дата и номер	Аннотация
1	Федеральный закон «Об информации, информационных технологиях и о защите информации»	27.07.2006 № 149-ФЗ	Регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, при применении информационных технологий, а также при обеспечении защиты информации, за исключением отношений, возникающих при охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.
2	Закон РФ «О государственной тайне»	21.07.1993 № 5485-1	Регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.
3	Федеральный закон от «О техническом регулировании»	27.12.2002 № 184-ФЗ	Регулирует отношения, возникающие при применении и исполнении на добровольной основе требований к продукции, процессам проектирования, оценке соответствия.
4	Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»	26.07.2017 №187-ФЗ	Регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.
5	Федеральный закон от «О персональных данных»	27.07.2006 № 152-ФЗ	Создает правовую основу обращения с персональными данными физических лиц в целях реализации конституционных прав человека, в том числе права на неприкосновенность частной жизни, личную и семейную тайну
6	Федеральный закон от «О коммерческой тайне»	29.07.20040 № 98-ФЗ	Регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности и предупреждением недобросовестной конкуренции. Действие Закона распространяется на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.
7	Федеральный закон «Об электронной подписи»	6.04.2011 № 63-ФЗ	Расширяет сферу использования и допустимые виды ЭП

Основные документы в области стандартизации (в соответствии с Федеральным законом «О стандартизации в Российской Федерации» от 29.06.2015 № 162-ФЗ)

№ п/п	Тип документа	Содержание документа
1	Документ по стандартизации	документ по стандартизации - документ, в котором для добровольного и многократного применения устанавливаются общие характеристики объекта стандартизации, а также правила и общие принципы в отношении объекта стандартизации, за исключением случаев, если обязательность применения документов по стандартизации устанавливается настоящим Федеральным законом
2	Национальный стандарт	документ по стандартизации, который разработан участником или участниками работ по стандартизации, по результатам экспертизы в техническом комитете по стандартизации или проектном техническом комитете по стандартизации утвержден федеральным органом исполнительной власти в сфере стандартизации и в котором для всеобщего применения устанавливаются общие характеристики объекта стандартизации, а также правила и общие принципы в отношении объекта стандартизации
3	Основополагающий национальный стандарт - национальный стандарт	Документ, разработанный и утвержденный федеральным органом исполнительной власти в сфере стандартизации, устанавливающий общие положения, касающиеся выполнения работ по стандартизации, а также виды национальных стандартов;
4	Рекомендации по стандартизации	документ национальной системы стандартизации, утвержденный федеральным органом исполнительной власти в сфере стандартизации и содержащий информацию организационного и методического характера, касающуюся проведения работ по стандартизации и способствующую применению соответствующего национального стандарта, либо положения, которые предварительно проверяются на практике до их установления в национальном стандарте или предварительном национальном стандарте
5	Свод правил	Документ по стандартизации, утвержденный федеральным органом исполнительной власти или Государственной корпорацией по атомной энергии "Росатом" и содержащий правила и общие принципы в отношении процессов в целях обеспечения соблюдения требований технических регламентов
6	Стандарт организации	Документ по стандартизации, утвержденный юридическим лицом, в том числе государственной корпорацией, саморегулируемой организацией, а также индивидуальным предпринимателем для совершенствования производства и обеспечения качества продукции, выполнения работ, оказания услуг
7	Технические условия	Вид стандарта организации, утвержденный изготовителем продукции или исполнителем работы, услуги

Технические комитеты по стандартизации

362	Защита информации	*Организация, ведущая секретариат ТК* Государственный научно - исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю (ГНИИИ ПТЗИ ФСТЭК России) *Председатель ТК* Куц Анатолий Владимирович Место работы: ФСТЭК России Должность: Заместитель директора ФСТЭК России *Коды областей стандартизации по ОКС* 01.040.01; 35.020; 35.040; 35.240.01 *Управление Росстандарта* Управление технического регулирования и стандартизации *НИИ системы Росстандарта* ФГУП "ВНИИНМАШ" *Документы национального органа по стандартизации, касающиеся организации и функционирования ТК* Приказ № 81/105 от 02.04.2002 ; Приказ № 294 от 05.02.2010 (утратил силу) Приказ № 406 от 01.06.2012 *Дата создания ТК* 01.04.2002

Технические комитеты по стандартизации

026	Криптографическая защита информации	*Организация, ведущая секретариат ТК* ОАО "ИнфоТеКС" *Председатель ТК* Кузьмин Алексей Сергеевич Место работы: Центр ФСБ России Должность: заместитель начальника Научная степень: доктор физико-математических наук, профессор *Коды областей стандартизации по ОКС* 35.040; 35.160 *Управление Росстандарта* Управление технического регулирования и стандартизации *НИИ системы Росстандарта* ФГУП "ВНИИНМАШ" *Документы национального органа по стандартизации, касающиеся организации и функционирования ТК* Приказ № 3825дсп от 28.12.2007; Приказ № 291 от 05.02.2010; Приказ № 4402 от 12.09.2011 *Дата создания ТК* 28.12.2007

Технические комитеты по стандартизации

022	Информационные технологии	*Организация, ведущая секретариат ТК* Учреждение Российской академии наук Институт проблем информатики (ИПИ РАН) *Председатель ТК* Головин Сергей Аанатольевич Место работы: Межотраслевой совет по техническому регулированию и стандартизации в сфере информационных технологий Должность: Председатель Научная степень: д.т.н., проф. *Коды областей стандартизации по ОКС* 03.080.99; 33.040.35; 33.050.30; 35.020; 35.040; 35.060; 35.080; 35.100.05; 35.100.10; 35.100.20; 35.100.30; 35.100.40; 35.100.60; 35.100.70; 35.110; 35.140; 35.160; 35.180; 35.200; 35.220.10; 35.220.20; 35.220.21; 35.220.22; 35.220.23; 35.240.15; 35.240.20; 35.240.30; 35.240.40; 35.240.60; 35.240.99; 35.260 *Коды продукции по ОКП* 401000; 402000; 403000; 404000; 405000; 406000; 408000; 421000; 422000; 423000; 425000; 426000; 427000; 428000; 501000; 502000; 503000; 50400; 505000; 506000; 507000; 508000; 509000 *Управление Росстандарта* Управление технического регулирования и стандартизации *НИИ системы Росстандарта* ФГУП "ВНИИНМАШ" *Документы национального органа по стандартизации, касающиеся организации и функционирования ТК* Приказ № 1/54 от 06.01.1995 (утратил силу) ; Приказ № 3702 от 19.10.2009 (Приложение 1 утратило силу) ; Приказ № 1728 от 13.05.2010 (утратил силу) ; Приказ № 734 от 7.09.2012 (утратил силу) ; Приказ № 389 от 31.03.2014 (утратил силу) ; Приказ № 463 от 22.04.2016 *Дата создания ТК* 06.01.95

Первые стандарты по информационной безопасности

Первым стандартом, получившим международное признание и оказавшим исключительно сильное влияние на последующие разработки в области информационной безопасности, стал стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем" (Department of Defense Trusted Computer System Evaliation Criteria, TCSEC, более известный (по цвету обложки) под названием "Оранжевая книга".

После "Оранжевой книги" была выпущена целая "Радужная серия". С концептуальной точки зрения, наиболее значимый документ в ней - "Интерпретация "Оранжевой книги" для сетевых конфигураций" (Trusted Network Interpretation).

Руководящие документы (РД) Гостехкомиссии России начали появляться несколько позже, и подтверждают разницу между автоматизированными системами (АС) и продуктами (средствами вычислительной техники, СВТ), но в общем и целом они долгое время следовали в фарватере "Оранжевой книги".

Первые стандарты по информационной безопасности

К ним относятся следующие документы:

1	Руководящий документ. Защита от несанкционированного доступа. Термины и определения. Утвержден решением председателя Гостехкомиссии России от 30.03.92
2	Руководящий документ. Защита от несанкционированного доступа. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 30.03.92
3	Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Утверждён решением председателя Гостехкомиссии России от 30.03.92
4	Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации. Утверждён решением председателя Гостехкомиссии России от 30.03.92
5	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 30.03.1992

Первые стандарты по информационной безопасности

Первое примечательное отклонение от этого курса произошло в 1997 году, когда был принят РД по отдельному сервису безопасности - межсетевым экранам (МЭ). Его основная идея - классифицировать МЭ на основании осуществляющих фильтрацию потоков данных уровней эталонной семиуровневой модели.

6	Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 25.07.97

Кроме вышеперечисленных РД были приняты ещё два документа:

7	Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Решение Председателя Гостехкомиссии России от 25.07.1997
8	Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом председателя Гостехкомиссии России от 4 июня 1999 г. № 114.

Наиболее важными из аспектами из Руководящих документов – является классификация автоматизированных систем по уровню защищенности от несанкционированного доступа и аналогичная классификация межсетевых экранов.

Критерии оценки безопасности информационных технологий

В 1990 году Рабочая группа 3 Подкомитета 27 Первого совместного технического комитета (JTC1/SC27/WG3) Международной организации по стандартизации (ISO) приступила к разработке "Критериев *оценки безопасности информационных технологий*" (Evaluation Criteria for IT Security, ECITS). Несколько позже, в 1993 году, правительственные организации шести североамериканских и европейских стран - Канады, США, Великобритании, Германии, Нидерландов и Франции - занялись составлением так называемых "*Общих критериев оценки безопасности информационных технологий*" (Common Criteria for IT Security Evaluation). За этим документом исторически закрепилось более короткое название - "*Общие критерии*", или ОК (Common Criteria, CC).

В качестве стратегического направления Гостехкомиссия России выбрала ориентацию на "Общие критерии". В 2002 году Гостехкомиссия России приняла в качестве РД русский перевод международного стандарта ISO/IEC 15408:1999 "Критерии оценки безопасности информационных технологий".

Критерии оценки безопасности информационных технологий

На сегодняшний день "Общие критерии" - самый полный и современный оценочный стандарт. Федеральным агентством по техническому регулированию и метрологии утверждены и введены в действие национальные стандарты:

- 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 15408-2-2012. Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ. Часть 2. Функциональные компоненты безопасности;
- ГОСТ Р ИСО/МЭК 15408-3-2012. Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ. Часть 3. Компоненты доверия к безопасности.

Критерии оценки безопасности информационных технологий

«Общие критерии» содержат два основных вида требований безопасности:

- *функциональные*, соответствующие активному аспекту защиты, предъявляемые к *функциям (сервисам) безопасности* и реализующим их механизмам;
- *требования доверия*, соответствующие пассивному аспекту; они предъявляются к технологии и процессу разработки и эксплуатации.

Требования безопасности формулируются, и их выполнение проверяется для определенного *объекта оценки* - аппаратно-программного продукта или *информационной системы*.

Безопасность в «Общих критериях» рассматривается не статично, а в соответствии с жизненным циклом *объекта оценки*. Кроме того, последний предстает в контексте среды безопасности, характеризующейся определенными условиями и угрозами.

Система стандартов РФ по защите информации

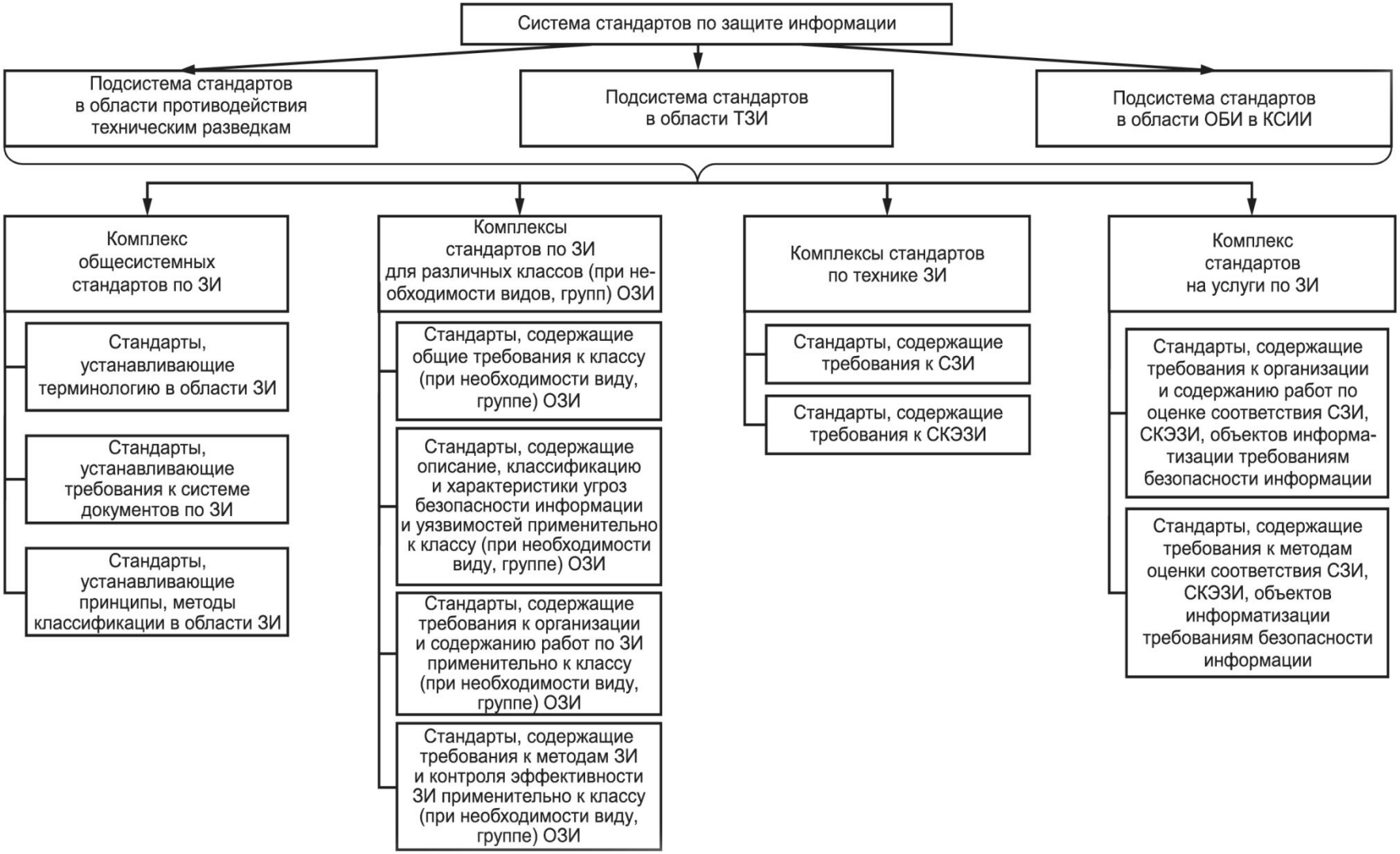
ГОСТ Р 52069.0-2013 «Защита информации. Система стандартов. Основные положения» устанавливает цель, задачи и структуру системы стандартов по защите (некриптографическими методами) информации, объекты и аспекты стандартизации в данной области.

Основными объектами стандартизации системы стандартов защиты информации являются:

- Защита информации как область деятельности:
  - противодействие техническим разведкам;
  - техническая защита информации;
  - обеспечение безопасности информации в ключевых системах информационной инфраструктуры;
- объекты защиты информации, в том числе:
  - промышленные объекты, объекты науки, энергетики, жизнеобеспечения;
  - объекты органов управления;
  - объекты информатизации;
  - продукция;
  - процессы (работы, технологии);
- угрозы безопасности информации и уязвимости объектов защиты информации;
- организация и содержание работ по защите информации;
- методы (процессы, работы, технологии) защиты информации и методы контроля состояния защиты информации;
- техника ЗИ, в том числе:
  - средства защиты информации;
  - средства контроля эффективности защиты информации;
- услуги по защите информации.

Система стандартов РФ по защите информации

Структура системы стандартов по защите информации



Системы менеджмента информационной безопасности

Семейство стандартов системы менеджмента серии 27000 представляют модель для создания, внедрения и функционирования системы менеджмента. Подкомитет SC 27 Совместного технического комитета ISO/IEC JTC 1 имеет в своем составе комиссию экспертов, которая работает в области создания системы международных стандартов по информационной безопасности, известной как семейство стандартов системы менеджмента информационной безопасности (СМИБ).

Стандарты устанавливают рекомендации по управлению информационной безопасностью лицам, ответственным за планирование, реализацию или поддержку решений безопасности в организации. Он предназначен для обеспечения общих основ для разработки стандартов безопасности и выбора практических мероприятий по управлению безопасностью в организации, а также в интересах обеспечения доверия в деловых отношениях между организациями.

Основой для разработки стандартов явился британский стандарт BS 7799 фактически имеющий статус международного (ISO/IEC 17799:2000 «Information technology. Code of practice for security management»).

Системы менеджмента информационной безопасности

Семейство стандартов системы менеджмента серии 27000 представляют модель для создания, внедрения и функционирования системы менеджмента. Подкомитет SC 27 Совместного технического комитета ISO/IEC JTC 1 имеет в своем составе комиссию экспертов, которая работает в области создания системы международных стандартов по информационной безопасности, известной как семейство стандартов системы менеджмента информационной безопасности (СМИБ).

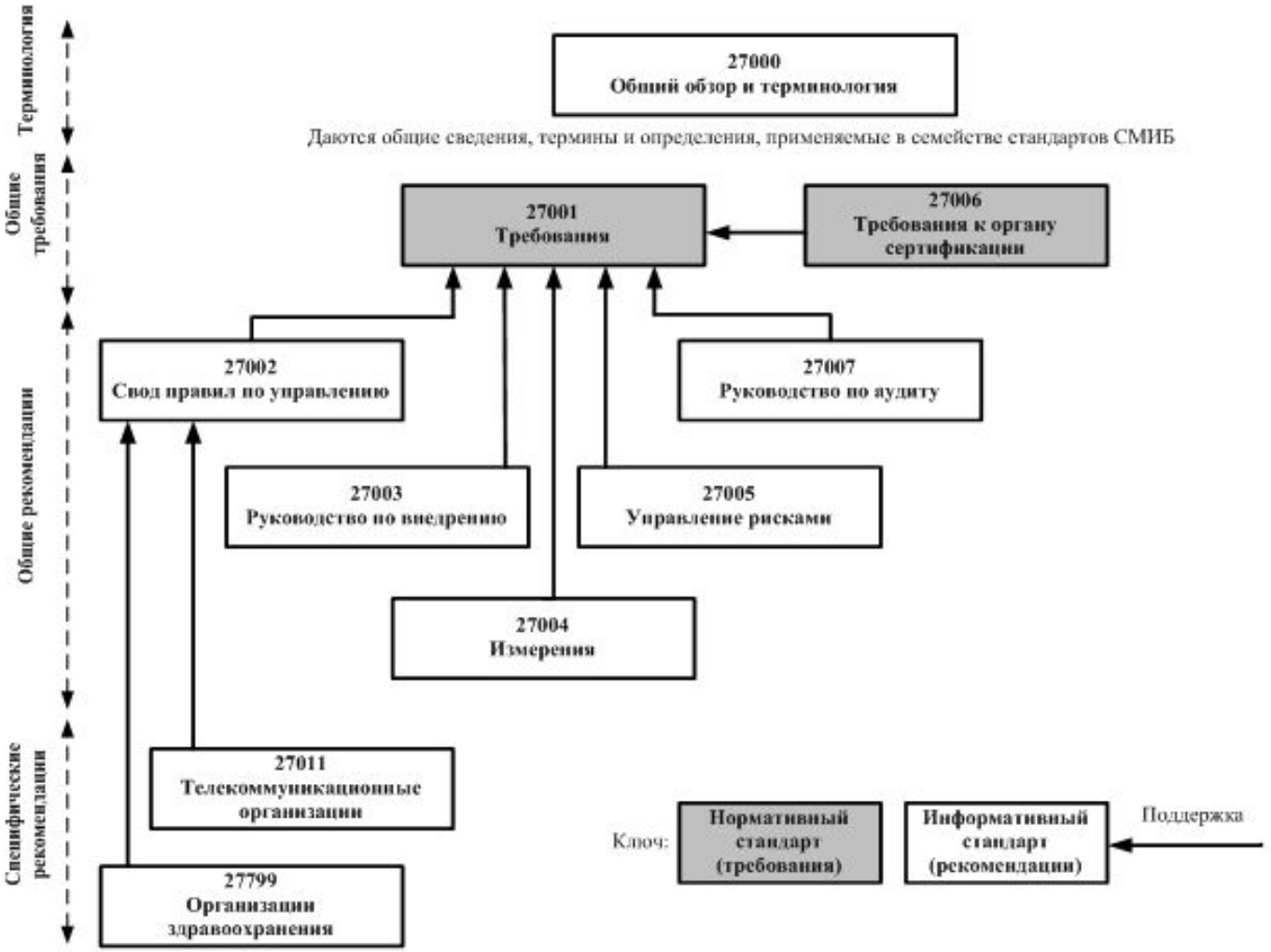
Основой для разработки стандартов явился британский стандарт BS 7799 фактически имеющий статус международного (ISO/IEC 17799:2000 «Information technology. Code of practice for security management»).

Семейство стандартов СМИБ содержит стандарты, которые:

- определяют требования к СМИБ и к сертификации таких систем;
- содержат прямую поддержку, детальное руководство и (или) интерпретацию полных процессов "План (Plan) - Осуществление (Do) -Проверка (Check) - Действие (Act)" (PDCA) и требования;
- включают в себя специальные руководящие принципы для СМИБ;
- руководят проведением оценки соответствия СМИБ.

Семейство стандартов СМИБ состоит из международных стандартов под общим названием Information technology – Security techniques (Информационные технологии. Методы и средства обеспечения безопасности).

Системы менеджмента информационной безопасности



Системы менеджмента информационной безопасности

Международный стандарт ISO/IEC 27000 содержит:

- обзор семейства стандартов СМИБ;
- введение в систему менеджмента информационной безопасности(СМИБ);
- краткое описание процесса "План (Plan) - Осуществление (Do) – Проверка (Check) - Действие (Act)" (PDCA);
- термины и определения для использования в семействе стандартов СМИБ.

Стандарты, задающие требования:

ISO/IEC 27001	**ISO/IEC 27006**
Информационная технология. Средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования	*Информационная технология. Средства обеспечения безопасности. Требования для органов, обеспечивающих аудит и сертификацию систем менеджмента информационной безопасности*
Определяет требования для создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшения документированной СМИБ в контексте общих деловых рисков организации. *Содержит нормативные требования для развертывания и функционирования СМИБ, включая набор средств управления для управления и уменьшения рисков, относящихся к информационным активам, которые организация стремится защитить.*	*Задает требования и является руководством для органов, проводящих аудит и сертификацию СМИБ на соответствие ISO/IEC 27001 в дополнение к требованиям, содержащимся в ISO/IEC 17021.* *Дополняет стандарт ISO/IEC 17021 в части требований для аккредитации органов сертификации, проводящих сертификацию соответствия требованиям, изложенным в стандарте ISO/IEC 27001.*

Стандарты по криптографической защите информации

Утвержденное Приказом ФСБ России от 9 февраля 2005 г. № 66 "Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации" (Положение ПКЗ-2005) рекомендует использовать при разработке средств криптографической защиты информации криптографические алгоритмы, утвержденные в качестве национальных стандартов.

С целью обеспечения деятельности по разработке криптографических стандартов и нормативных документов, регламентирующих их применение, Приказом Ростехрегулирования от 28 декабря 2007 г. был создан технический комитет по стандартизации "Криптографическая защита информации", получивший сокращенное наименование ТК 26.

В настоящее время действует пять национальных стандартов в области криптографической защиты информации:

- ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования;
- ГОСТ Р 34.10-2012. Информационная технология. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Процессы формирования и проверки электронной цифровой подписи;
- ГОСТ Р 34.11-2012. Информационная технология. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Функция хэширования;
- ГОСТ Р 34.12-2015. Информационная технология. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Блочные шифры
- ГОСТ Р 34.13-2015 Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров

Стандарты информационной безопасности в кредитно-финансовой сфере

В настоящий момент приняты и введены в действие распоряжением Банка России следующие стандарты (совокупность указанных документов принято называть **Комплексом БР ИББС**):

- СТО БР ИББС-1.0-2014. «Общие положения (5 редакция)».
- СТО БР ИББС-1.1-2007. «Аудит информационной безопасности».
- СТО БР ИББС-1.2-2014. «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014 (4 редакция)».
- СТО БР ИББС-1.3-2016 «Сбор и анализ технических данных при выявлении и расследовании инцидентов информационной безопасности при осуществлении переводов денежных средств».
- СТО БР ИББС-1.4-2018 «Управление риском информационной безопасности при аутсорсинге»

Стандарты информационной безопасности в кредитно-финансовой сфере

Кроме того, Банком России разработаны и введены следующие рекомендации в области стандартизации:

- РС БР ИББС-2.0-2007. «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствие с требованиями СТО БР ИББС-1.0».
- РС БР ИББС-2.1-2007. «Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».
- РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности».
- РС БР ИББС-2.5-2014. «Менеджмент инцидентов информационной безопасности».
- РС БР ИББС-2.6-2014. «Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем».
- РС БР ИББС-2.7-2015. «Ресурсное обеспечение информационной безопасности».
- РС БР ИББС-2.8-2015. «Обеспечение информационной безопасности при использовании технологии виртуализации».
- РС БР ИББС-2.9-2016. «Предотвращение утечек информации».

Стандарты информационной безопасности в кредитно-финансовой сфере

Для реализации и поддержания системы обеспечения информационной безопасности (СОИБ) реализуются следующие группы процессов:

— планирование СОИБ организации БС РФ (“планирование”);

— реализация СОИБ организации БС РФ (“реализация”);

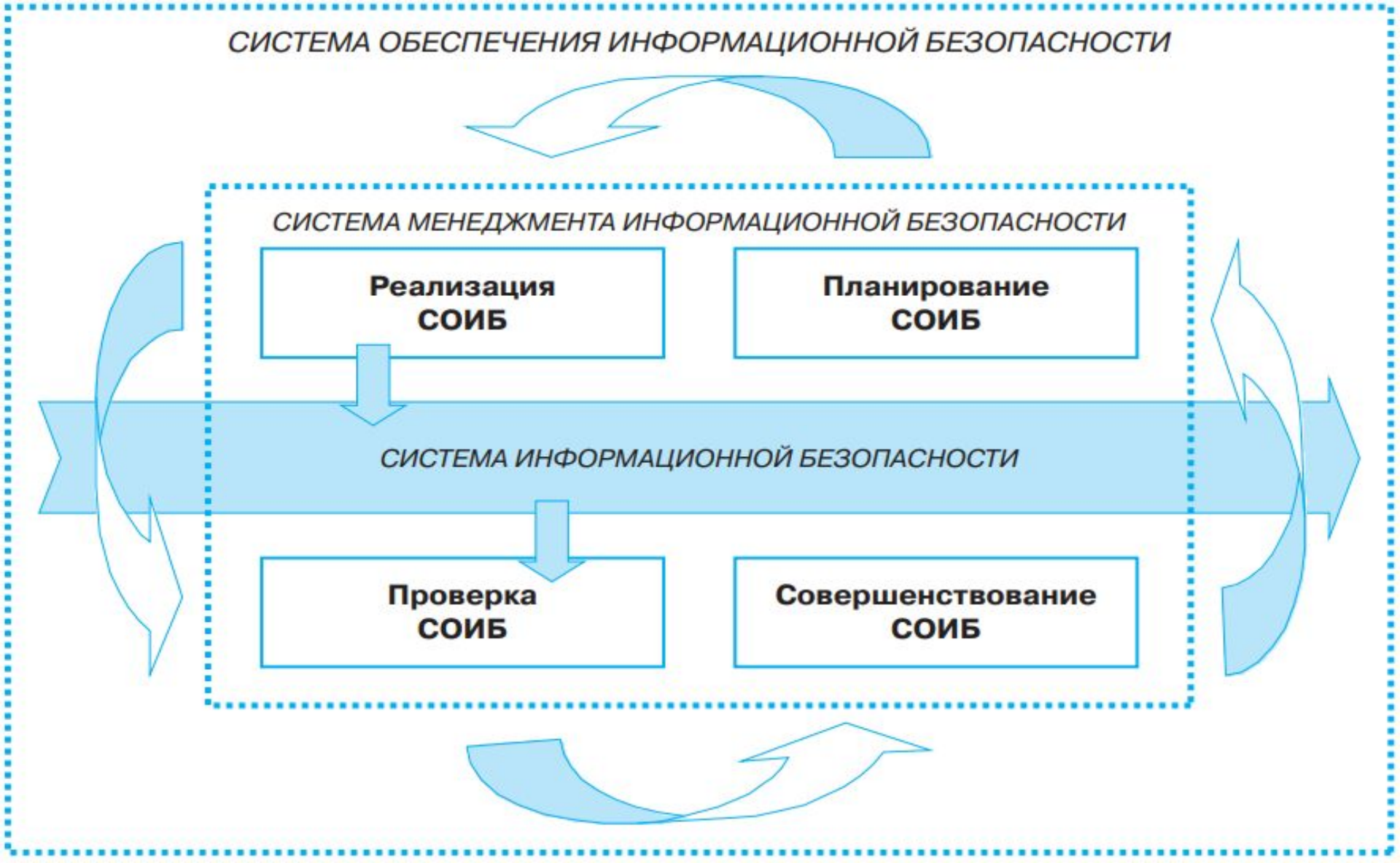
— мониторинг и анализ СОИБ организации БС РФ (“проверка”);

—поддержка и улучшение СОИБ организации БС РФ (“совершенствование”).

Указанные группы процессов составляют СМИБ организации БС РФ. Менеджмент ИБ есть часть общего корпоративного менеджмента организации БС РФ, которая ориентирована на содействие достижению целей деятельности организации через обеспечение защищенности ее информационной сферы.

Группы процессов СМИБ организации БС РФ рекомендуется организовывать в виде циклической модели Деминга “… — планирование — реализация — проверка — совершенствование — планирование — …”, которая является основой модели менеджмента стандартов качества ГОСТ Р ИСО 9001 и ИБ ISO/IEC IS 27001-2005.

Стандарты информационной безопасности в кредитно-финансовой сфере



Обеспечение безопасности критической информационной инфраструктуры Российской Федерации

Целью государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации, согласно документу «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации», утв. Президентом Российской Федерации Д. Медведевым 3 февраля 2012 г., № 803, является снижение до минимально возможного уровня рисков неконтролируемого вмешательства в процессы функционирования данных систем, а также минимизация негативных последствий подобного вмешательства. Требования к безопасности КИИ РФ приведены в таких документах как:

- Приказ ФСТЭК России от 25 декабря 2017 г. N 239 Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации
- Приказ ФСТЭК России от 21 декабря 2017 г. N 235 Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования
- Приказ ФСБ России от 24 июля 2018 г. N 366 О национальном координационном центре по компьютерным инцидентам.

Перечень национальных стандартов по информационной безопасности

ГОСТ Р ИСО/МЭК 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 7498-4-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 4. Основы административного управления
ГОСТ Р ИСО 7498-3-97	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 3. Присвоение имен и адресация

Перечень национальных стандартов по информационной безопасности

Общие критерии оценки безопасности информационных технологий	
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
Системы менеджмента информационной безопасности	
ГОСТ Р ИСО/МЭК 27000-2012	Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
ГОСТ Р ИСО/МЭК 27001-2006	Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
ГОСТ Р ИСО/МЭК 27002-2012	Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Свод норм и правил менеджмента информационной безопасности

Перечень национальных стандартов по информационной безопасности

Системы менеджмента информационной безопасности	
ГОСТ Р ИСО/МЭК 27003-2012	Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.
ГОСТ Р ИСО/МЭК 27004-2011	Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.
ГОСТ Р ИСО/МЭК 27005-2010	Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Менеджмент риска информационной безопасности.
ГОСТ Р ИСО/МЭК 27006-2008	Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.
ГОСТ Р ИСО/МЭК 27007-2014	Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.
ГОСТ Р 56045-2014/ISO/IEC TR 27008:2011	Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью.
ГОСТ Р ИСО/МЭК 27011-2012	Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002
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. Information technology. Security techniques. Part 1. Concepts and models for information and communications technology security management.

Перечень национальных стандартов по информационной безопасности

Системы менеджмента информационной безопасности	
ГОСТ Р ИСО/МЭК ТО 13335-5-2006	Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети. Information technology. Security techniques. Part 5. Management quidance on network security.
ГОСТ Р ИСО/МЭК 27031-2012	Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса
ГОСТ Р ИСО/МЭК 27033-1-2011	Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции
ГОСТ Р ИСО/МЭК 27033-3-2014	Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления.
ГОСТ Р ИСО/МЭК 15026-2002	Информационная технология. Уровни целостности систем и программных средств. Information technology. System and software integrity levels.
ГОСТ Р ИСО/МЭК 13569-2007	Финансовые услуги. Рекомендации по информационной безопасности. Financial services — Information security Guidelines.
ГОСТ Р ИСО/МЭК ТО 18044-2007	Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Information technology. Security techniques. Information security incident management.
ГОСТ Р ИСО/МЭК 18045-2008	Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. Information technology. Security techniques. Methodology for IT security evaluation.

Перечень национальных стандартов по информационной безопасности

Системы менеджмента информационной безопасности	
ГОСТ Р 51275-2006	Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Protection of information. Object of informatisation. Factors influencing the information. General.
ГОСТ Р 50739-95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Computers technique. Information protection against unauthorised access to information. General technical requirements.
ГОСТ Р 51188-98	Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Information security. Software testing for the existence of computer viruses. The sample manual.
Р 50.1.056	Техническая защита информации. Основные термины и определения.
ГОСТ Р 50922-2006	Защита информации. Основные термины и определения. Protection of information. Basic terms and definitions.
ГОСТ 51583-2000	Порядок создания автоматизированных систем в защищенном исполнении.
ГОСТ Р 51624-2000	Автоматизированные системы в защищенном исполнении. Общие положения.
ГОСТ Р 52447-2005	Защита информации. Техника защиты информации. Номенклатура показателей качества. Information protection. Information protection technology. Nomenclature of quality indices.

Перечень национальных стандартов по информационной безопасности

Системы менеджмента информационной безопасности	
ГОСТ Р 52069.0-2003	Защита информации. Система стандартов. Основные положения. Safety of information. System of standards. Basic principles.
ГОСТ Р ИСО/МЭК 19794-2-2005	Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца - контрольные точки. Automatic identification. Biometrics. Biometric data interchange formats. Part 2. Finger minutiae data.
ГОСТ Р ИСО/МЭК 19794-4-2006	Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца. Automatic identification. Biometrics. Biometric data interchange formats. Part 4. Finger image data.
ГОСТ Р ИСО/МЭК 19794-5-2006	Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица. Automatic identification. Biometrics. Biometric data interchange formats. Part 5. Face image data.
ГОСТ Р ИСО/МЭК 19794-6-2006	Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза. Automatic identification. Biometrics. Biometric data interchange formats. Part 6. Iris image data.
ГОСТ Р 51725.6-2002	Каталогизация продукции для федеральных государственных нужд. Сети телекоммуникационные и базы данных. Требования информационной безопасности. Catalogization of products for federal state needs. Telecommunication networks and data bases. Requirements of information security.
ГОСТ Р 51898-2002	Аспекты безопасности. Правила включения в стандарты. Safety aspects. Guidelines for their inclusion in standards.

Перечень национальных стандартов по информационной безопасности

Стандарты по криптографической защите информации	
ГОСТ 28147-89	Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
ГОСТ Р 34.10-2001	Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Information technology. Cryptographic data security. Formation and verification processes of [electronic] digital signature.
ГОСТ Р 34.11-94	Информационная технология. Криптографическая защита информации. Функция хэширования. Information technology. Cryptographic data security. Hashing function.
ГОСТ 34.311-95	Информационная технология. Криптографическая защита информации. Функция хэширования. Information technology. Cryptographic Data Security. Cashing function.

Перечень национальных стандартов по информационной безопасности

Стандарты информационной безопасности в кредитно-финансовой сфере	
СТО БР ИББС-1.0-2014	Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения
СТО БР ИББС-1.1-2007	Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности.
СТО БР ИББС-1.2-2010	Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-20xx
РС БР ИББС-2.0-2007	Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0.
РС БР ИББС-2.1-2007	Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0.
РС БР ИББС-2.2-2009	Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ.
РС БР ИББС-2.3-2010	Обеспечение ИБ организаций банковской системы РФ. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы РФ
РС БР ИББС-2.4-2010	Обеспечение ИБ организаций банковской системы РФ. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах ПД организаций банков банковской системы РФ
	Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях БС РФ, разработанные совместно Банком России, АРБ и Ассоциацией региональных банков России (Ассоциацией «Россия»)